Procurement & Contracts
Office of Facilities & Procurement Management
900 S.W. Jackson St., Room 451 South
Topeka, KS 66612

Kansas
Department of Administration

Phone: (785) 296-2376
Fax: (785) 296-7240
http://admin.ks.gov/offices/procurement-and-contracts

Jim Clark, Secretary

Sam Brownback, Governor

# REQUEST FOR PROPOSAL (RFP)

**Bid Event Number:** EVT0003605
**Requisition ID:** 0000025826
**Document Number:** RFX0000574
**Replaces Contract:** N/A
**Date Posted:** March 11, 2015
**Closing Date:** April 9, 2015, 2:00 PM

**Procurement Officer:** Neal Farron
**Telephone:** 785/296-3122
**E-Mail Address:** Neal.Farron@da.ks.gov
**Web Address:** http://admin.ks.gov/offices/procurement-and-contracts/

**Agency:** Kansas Dept. of Health and Environment - 26400
**Item:** Software, Mass Notification / Communication

**Period of Contract:** Date of Award for One Year
(with the option to renew for three (3) additional 12 month maintenance periods)

**Bid Guarantee:** No monetary bid guarantee required.

---

This Bid Event was recently posted to the Procurement and Contracts Internet website.
The document can be downloaded by going to the following website:

http://admin.ks.gov/offices/procurement-and-contracts/

**It shall be the bidder's responsibility to monitor this website on a regular basis for any changes/amendments.**

# SIGNATURE SHEET

**Item:** Software, Mass Notification / Communication
**Agency:** Kansas Dept. of Health and Environment - 26400
**Closing Date:** April 9, 2015, 2:00 PM

By submission of a bid and the signatures affixed thereto, the bidder certifies all products and services proposed in the bid meet or exceed all requirements of this specification as set forth in the request and that all exceptions are clearly identified.
Legal Name of Person, Firm or Corporation____

Mailing Address City & State __ Zip __

Toll Free Telephone ___ Local

Cell Phone ____ Fax Number _

Tax Number __

CAUTION: If your tax number is the same as your Social Security Number (SSN), you must leave this line blank. DO NOT enter your SSN on this signature sheet. If your SSN is required to process a contract award, including any tax clearance requirements, you will be contacted by an authorized representative of the Office of Procurement and Contracts at a later date.

E-Mail

Signature _____ Date __

Typed Name __ Title __

In the event the **contact for the bidding process** is different from above, indicate contact information below.

**Bidding Process** Contact Name _____

Mailing Address _____ City & State __ Zip ___

Toll Free Telephone ___ Local

Cell Phone ____ Fax Number _

E-Mail

If **awarded a contract and purchase orders** are to be directed to an address other than above, indicate mailing address and telephone number below.

**Award** Contact Name _

Mailing Address _____ City & State __ Zip ___

Toll Free Telephone ___ Local

Cell Phone ____ Fax Number _

E-Mail

## 1. Bidding Instructions

### 1.1. Bid Event ID / Reference Number

The Bid Event ID / RFP number, indicated in the header of this page, as well as on the first page of this proposal, has been assigned to this RFP and MUST be shown on all correspondence or other documents associated with this RFP and MUST be referred to in all verbal communications. All inquiries, written or verbal, shall be directed only to the procurement officer reflected on Page 1 of this proposal. There shall be no communication with any other State employee regarding this RFP except with designated state participants in attendance ONLY DURING:

- Negotiations
- Contract Signing
- as otherwise specified in this RFP.

Violations of this provision by bidder or state agency personnel may result in the rejection of the proposal.

### 1.2. Questions/Addenda

Questions requesting clarification of the bid event must be submitted in WRITING to the Procurement Officer prior to the close of business on March 25, 2015 to the following address:

Neal Farron
**Telephone:** 785/296-3122
**Facsimile:** 785-296-7240
**E-Mail Address:** Neal.Farron@da.ks.gov

Kansas Department of Administration
Procurement and Contracts
900 SW Jackson, Suite 451-South
Topeka, KS 66612-1286

Failure to notify the Procurement Officer of any conflicts or ambiguities in this bid event may result in items being resolved in the best interest of the State. Any modification to this bid event shall be made in writing by addendum and mailed to all vendors who received the original request. Only Written communications are binding.

Answers to questions will be available in the form of an addendum on the Procurement and Contracts' website, http://admin.ks.gov/offices/procurement-and-contracts.

It shall be the responsibility of all participating bidders to acquire any and all addenda and additional information as it is made available from the web site cited above. Vendors/Bidders not initially invited to participate in this Bid Event must notify the Procurement Officer (Event Contact) of their intent to bid at least 24 hours prior to the event's closing date/time. Bidders are required to check the website periodically for any additional information or instructions.

### 1.3. Pre-Bid Conference

No pre-bid conference is scheduled for this bid event.

### 1.4. Negotiated Procurement

This is a negotiated procurement pursuant to K.S.A. 75-37,102. Final evaluation and award will be made by the Procurement Negotiation Committee (PNC) consisting of the following entities (or their designees):

- Secretary of Department of Administration;
- Director of Purchases, Department of Administration; and
- Head of Using Agency

### 1.5. Appearance Before Committee

Any, all or no bidders may be required to appear before the PNC to explain the bidder's understanding and approach to the project and/or respond to questions from the PNC concerning the proposal; or, the PNC may award without conducting negotiations, based on the initial proposal. The PNC reserves the right to request information from bidders as needed. If information is requested, the PNC is not required to request the information of all bidders.

Bidders selected to participate in negotiations may be given an opportunity to submit a revised technical and/or cost proposal/offer to the PNC, subject to a specified cut off time for submittal of revisions. Meetings before the PNC are not subject to the Open Meetings Act. Bidders are prohibited from electronically recording these meetings. All information received prior to the cut off time will be considered part of the bidder's revised offer.

No additional revisions shall be made after the specified cut off time unless requested by the PNC.

### 1.6. Notices

All notices, demands, requests, approvals, reports, instructions, consents or other communications (collectively "notices") that may be required or desired to be given by either party to the other shall be IN WRITING and addressed as follows:

Kansas Department of Administration
Procurement and Contracts
900 SW Jackson, Suite 451-South
Topeka, Kansas 66612-1286

RE: EVT0003605

or to any other persons or addresses as may be designated by notice from one party to the other.

### 1.7. Cost of Preparing Proposal

The cost of developing and submitting the proposal is entirely the responsibility of the bidder. This includes costs to determine the nature of the engagement, preparation of the proposal, submitting the proposal, negotiating for the contract and other costs associated with this RFP.

### 1.8. Preparation of Proposal

Prices are to be entered in spaces provided on the cost proposal form if provided herein. Computations and totals shall be indicated where required. In case of error in computations or totals, the unit price shall govern. The PNC has the right to rely on any prices provided by bidders. The bidder shall be responsible for any mathematical errors. The PNC reserves the right to reject proposals which contain errors.

All copies of cost proposals shall be submitted in a separate sealed envelope or container separate from the technical proposal. The outside shall be identified clearly as "Cost Proposal" or "Technical Proposal" with the Bid Event ID / RFP number and closing date.

A proposal shall not be considered for award if the price in the proposal was not arrived at independently and without collusion, consultation, communication or agreement as to any matter related to price with any other bidder, competitor or public officer/employee.

Technical proposals shall contain a concise description of bidder's capabilities to satisfy the requirements of this RFP with emphasis on completeness and clarity of content. Repetition of terms and conditions of the RFP without additional clarification shall not be considered responsive.

### 1.9. Signature of Proposals

Each proposal shall give the complete legal name and mailing address of the bidder and be signed by an authorized representative by original signature with his or her name and legal title typed below the signature line. If the contract's contact will be a different entity, indicate that individual's contact information for communication purposes. Each proposal shall include the bidder's tax number.

### 1.10. Acknowledgment of Amendments

All bidders shall acknowledge receipt of any amendments to this bid event by returning a signed hard copy with the bid. Failure to acknowledge receipt of any amendments may render the proposal to be non-responsive. Changes to this bid event shall be issued only by the Office of Procurement and Contracts in writing.

### 1.11. Modification of Proposals

A bidder may modify a proposal by letter or by FAX transmission at any time prior to the closing date and time for receipt of proposals.

### 1.12. Withdrawal of Proposals

A proposal may be withdrawn on written request from the bidder to the Procurement Officer at the Office of Procurement and Contracts prior to the closing date.

### 1.13. Competition

The purpose of this bid event is to seek competition. The bidder shall advise the Office of Procurement and Contracts if any specification, language or other requirement inadvertently restricts or limits bidding to a single source. Notification shall be in writing and must be received by the Office of Procurement and Contracts no later than five (5) business days prior to the bid closing date. The Director of Purchases reserves the right to waive minor deviations in the specifications which do not hinder the intent of this bid event.

### 1.14. Evaluation of Proposals

Award shall be made in the best interest of the State as determined by the PNC or their designees. Although no weighted value is assigned, consideration may focus toward but is not limited to:

- Cost. Bidders are not to inflate prices in the initial proposal as cost is a factor in determining who may receive an award or be invited to formal negotiations. The State reserves the right to award to the lowest responsive bid without conducting formal negotiations, if authorized by the PNC.
- Adequacy and completeness of proposal
- Bidder's understanding of the project
- Bidder's qualifications and experience in delivering solution
- Bidder's understanding of the services to be delivered
- Compliance with the terms and conditions of the RFP
- Experience in providing like services
- Qualified staff
- Methodology to accomplish tasks
- Response format as required by this RFP
- Ability to meet requirements
- Demonstration of software as a service

### 1.15. Acceptance or Rejection

The Committee reserves the right to accept or reject any or all proposals or part of a proposal; to waive any informalities or technicalities; clarify any ambiguities in proposals; modify any criteria in this RFP; and unless otherwise specified, to accept any item in a proposal.

### 1.16. Proposal Disclosures

At the time of closing, only the names of those who submitted proposals shall be made public information. No price information will be released. A List of Bidders may be obtained in the following manner:

1. Attending the public bid opening at the time and date noted on the Bid Event, OR
2. Requesting a List of Bidders via E-mail to tabsheets@da.ks.gov or in writing to the following address. Include the Bid Event number EVT0003605 in all requests.

Kansas Department of Administration
Procurement and Contracts
Attn: Bid Results
900 SW Jackson, Suite 451-South
Topeka, KS 66612-1286

All other documents pertaining to the bid (tabsheet, individual bids, proposals, contract, etc.) are not available until the bid has been awarded, contract executed or all bids rejected.

Once a bid file is available, a request for a cost estimate may be submitted to the e-mail or address noted above for the costs associated with the reproduction of bid documents. Procurement and Contracts will attempt to provide all Open Records requests with electronic copies when possible.

Requests will not be fulfilled until payment has been received.

Documents will be sent via First Class Mail. If requested, they may be sent via express mail services at the expense of the requester.

Any questions regarding Open Records requests for bid results should be directed to tabsheets@da.ks.gov or 785-296-0002.

### 1.17. Disclosure of Proposal Content and Proprietary Information

All proposals become the property of the State of Kansas. The Open Records Act (K.S.A. 45-215 et seq) of the State of Kansas requires public information be placed in the public domain at the conclusion of the selection process, and be available for examination by all interested parties. (http://www.admin.ks.gov/offices/chief-counsel/kansas-open-records-act/kansas-open-records-act-procurement-and-contracts) No proposals shall be disclosed until after a contract award has been issued. The State reserves the right to destroy all proposals if the RFP is withdrawn, a contract award is withdrawn, or in accordance with Kansas law. Late Technical and/or Cost proposals will be retained unopened in the file and not receive consideration or may be returned to the bidder.

Trade secrets or proprietary information legally recognized as such and protected by law may be requested to be withheld if clearly labeled "Proprietary" on each individual page and provided as separate from the main proposal. Pricing information is not considered proprietary and the bidder's entire proposal response package will not be considered proprietary.

All information requested to be handled as "Proprietary" shall be submitted separately from the main proposal and clearly labeled, in a separate envelope or clipped apart from all other documentation. The bidder shall provide detailed written documentation justifying why this material should be considered "Proprietary". The Office of Procurement and Contracts reserves the right to accept, amend or deny such requests for maintaining information as proprietary in accordance with Kansas law.

The State of Kansas does not guarantee protection of any information which is not submitted as required.

### 1.18. Exceptions

By submission of a response, the bidder acknowledges and accepts all terms and conditions of the RFP unless clearly avowed and wholly documented in a separate section of the Technical Proposal to be entitled: "Exceptions".

### 1.19. Notice of Award

An award is made on execution of the written contract by all parties.

### 1.20. News Releases

Only the State is authorized to issue news releases relating to this bid event, its evaluation, award and/or performance of the resulting contract.

## 2. Proposal Response

### 2.1. Submission of Proposals

Bidder's proposal shall consist of:

- One (1) original and 4 copies of the Technical Proposal, including the signed Event Details document, applicable literature and other supporting documents;
- One (1) original and 4 copies of the cost proposal including the signed Event Details document,
- 3 electronic / software version(s) of the technical and cost proposals are required. This shall be provided on flash drives, in Microsoft® Word, Excel or searchable PDF®. Technical and cost responses shall be submitted on drives (6 total).

All copies of cost proposals shall be submitted in a separate sealed envelope or container separate from the technical proposal. The outside shall be identified clearly as "Cost Proposal" or "Technical Proposal" with the Bid Event ID number and closing date.

Bidder's proposal, sealed securely in an envelope or other container, shall be received no later than 2:00 p.m., Central Time, on the closing date, addressed as follows:

Kansas Department of Administration
Procurement and Contracts
Proposal #: EVT0003605
Closing Date: March 31, 2015
900 SW Jackson Street, Suite 451-South
Topeka, KS 66612-1286

It is the bidder's responsibility to ensure bids are received by the closing date and time. Delays in mail delivery or any other means of transmittal, including couriers or agents of the issuing entity shall not excuse late bid submissions.

Faxed, e-mailed or telephoned proposals are not acceptable unless otherwise specified.

Proposals received prior to the closing date shall be kept secured and sealed until closing. The State shall not be responsible for the premature opening of a proposal or for the rejection of a proposal that was not received prior to the closing date because it was not properly identified on the outside of the envelope or container. Late Technical and/or Cost proposals will be retained unopened in the file and not receive consideration or may be returned to the bidder.

### 2.2. Proposal Format

Bidders are instructed to prepare their Technical Proposal following the same sequence as this RFP.

### 2.3. Transmittal Letter

All bidders shall respond to the following statements:

(a) the bidder is the prime contractor and identifying all subcontractors;
(b) the bidder is a corporation or other legal entity;
(c) no attempt has been made or will be made to induce any other person or firm to submit or not to submit a proposal;
(d) the bidder does not discriminate in employment practices with regard to race, color, religion, age (except as provided by law), sex, marital status, political affiliation, national origin or disability;
(e) no cost or pricing information has been included in the transmittal letter or the Technical Proposal;
(f) the bidder presently has no interest, direct or indirect, which would conflict with the performance of services under this contract and shall not employ, in the performance of this contract, any person having a conflict;
(g) the person signing the proposal is authorized to make decisions as to pricing quoted and has not participated, and will not participate, in any action contrary to the above statements;
(h) whether there is a reasonable probability that the bidder is or will be associated with any parent, affiliate or subsidiary organization, either formally or informally, in supplying any service or furnishing any supplies or equipment to the bidder which would relate to the performance of this contract. If the statement is in the affirmative, the bidder is required to submit with the proposal, written certification and authorization from the parent, affiliate or subsidiary organization granting the State and/or the federal government the right to examine any directly pertinent books, documents, papers and records involving such transactions related to the contract. Further, if at any time after a proposal is submitted, such an association arises, the bidder will obtain a similar certification and authorization and failure to do so will constitute grounds for termination for cause of the contract at the option of the State;

(i) bidder agrees that any lost or reduced federal matching money resulting from unacceptable performance in a contractor task or responsibility defined in the RFP, contract or modification shall be accompanied by reductions in state payments to Contractor; and
(j) the bidder has not been retained, nor has it retained a person to solicit or secure a state contract on an agreement or understanding for a commission, percentage, brokerage or contingent fee, except for retention of bona fide employees or bona fide established commercial selling agencies maintained by the bidder for the purpose of securing business.

For breach of this provision, the Committee shall have the right to reject the proposal, terminate the contract for cause and/or deduct from the contract price or otherwise recover the full amount of such commission, percentage, brokerage or contingent fee or other benefit.

### 2.4. Bidder Information

The bidder must include a narrative of the bidder's corporation and each subcontractor if any. The narrative shall include the following:

(a) date established;
(b) ownership (public, partnership, subsidiary, etc.);
(c) number of personnel, full and part time, assigned to this project by function and job title;
(d) resources assigned to this project and the extent they are dedicated to other matters;
(e) organizational chart;
(f) financial statement may be required.

### 2.5. Qualifications

A description of the bidder's qualifications and experience providing the requested or similar service shall be submitted with the Technical Proposal. The bidder must be an established firm recognized for its capacity to perform. The bidder must have sufficient personnel to meet the deadlines specified in the bid event.

### 2.6. Experience

All bidders are preferred to have a minimum of 2 years continuous active participation in the applicable industry, providing equipment/services comparable in size and complexity to those specified herein.

### 2.7. Timeline

A timeline for implementing services must be submitted with the bid.

### 2.8. Methodology

Bidders shall submit with the bid, a detailed explanation of the methodology for implementing services.

### 2.9. References

Provide (3) references who have purchased similar items or services from the bidder in the last 2 year(s). References shall show firm name, contact person, address, e-mail address and phone number. Bidder's employees and the buying agency shall not be shown as references.

### 2.10. Bidder Contracts

Bidders must include with their RFP response, a copy of any contracts, agreements, licenses, warranties, etc. that the bidder would propose to incorporate into the contract generated from this Bid Event. (State of Kansas form DA-146a remains a mandatory requirement in all contracts.)

### 2.11. Alternate Proposals/Equivalent Items

Bids on goods and services comparable to those specified herein are invited. Whenever a material, article or piece of equipment is identified in the specifications by reference to a manufacturer's or vendor's name, trade name, catalog number, etc., it is intended to establish a standard, unless otherwise specifically stated. Any material, article or equipment of other manufacturers or vendors shall perform to the standard of the item specified. Equivalent bids must be accompanied by sufficient descriptive literature and/or specifications to provide for detailed comparison. Samples of items, if required, shall be furnished at no expense to the State and if not destroyed in the evaluation process, shall be returned at bidder's expense, if requested.

The State of Kansas reserves the right to determine and approve or deny "equivalency" in comparison of alternate bids.

### 2.12. Technical Literature

All Technical Proposals shall include specifications and technical literature sufficient to allow the State to determine that the equipment/services meet(s) all requirements. If a requirement is not addressed in the technical literature, it must be supported by additional documentation and included with the bid. Proposals without sufficient technical documentation may be rejected.

### 2.13. Unit Pricing

Each item required by the bid must be individually priced (i.e. priced per single unit) and be able to be ordered individually.

### 2.14. Equipment

All proposed equipment, equipment options, and hardware expansions must be identified by manufacturer and model number and descriptive literature of such equipment must be submitted with the bid response.

### 2.15. Procurement Card (P-Card)

Many State Agencies use a State of Kansas Procurement Card (currently Visa) in lieu of a state warrant to pay for certain purchases. No additional charges will be allowed for using the P-Card. Bidders shall indicate on the Event Details document if they will accept the Procurement Card for payment.

## 3. Terms and Conditions

### 3.1. Contract
The successful bidder will be required to enter into a written contract with the State. The contractor agrees to accept the provisions of Form DA 146a (Contractual Provisions Attachment), which is incorporated into all contracts with the State and is incorporated into this bid event.

### 3.2. Contract Documents
This bid event, any amendments, the response and any response amendments of the Contractor, and the State of Kansas DA-146a (Contractual Provision Attachment) shall be incorporated into the written contract, which shall compose the complete understanding of the parties.

In the event of a conflict in terms of language among the documents, the following order of precedence shall govern:

- Form DA 146a;
- written modifications to the executed contract;
- written contract signed by the parties;
- the Bid Event documents, including any and all amendments; and
- Contractor's written offer submitted in response to the Bid Event as finalized.

### 3.3. Captions
The captions or headings in this contract are for reference only and do not define, describe, extend, or limit the scope or intent of this contract.

### 3.4. Definitions
A glossary of common procurement terms is available at http://admin.ks.gov/offices/procurement-and-contracts, under the "Procurement Forms" link.

### 3.5. Contract Formation
No contract shall be considered to have been entered into by the State until all statutorily required signatures and certifications have been rendered and a written contract has been signed by the contractor.

### 3.6. Statutes
Each and every provision of law and clause required by law to be inserted in the contract shall be deemed to be inserted herein and the contract shall be read and enforced as though it were included herein. If through mistake or otherwise any such provision is not inserted, or is not correctly inserted, then on the application of either party the contract shall be amended to make such insertion or correction.

### 3.7. Governing Law
This contract shall be governed by the laws of the State of Kansas and shall be deemed executed in Topeka, Shawnee County, Kansas.

### 3.8. Jurisdiction
The parties shall bring any and all legal proceedings arising hereunder in the State of Kansas District Court of Shawnee County, unless otherwise specified and agreed upon by the State of Kansas. Contractor waives personal service of process, all defenses of lack of personal jurisdiction and forum non conveniens. The Eleventh Amendment of the United States Constitution is an inherent and incumbent protection with the State of Kansas and need not be reserved, but prudence requires the State to reiterate that nothing related to this Agreement shall be deemed a waiver of the Eleventh Amendment

### 3.9. Mandatory Provisions
The provisions found in Contractual Provisions Attachment (DA 146a) are incorporated by reference and made a part of this contract.

### 3.10. Termination for Cause
The Director of Purchases may terminate this contract, or any part of this contract, for cause under any one of the following circumstances:

- the Contractor fails to make delivery of goods or services as specified in this contract;
- the Contractor provides substandard quality or workmanship;
- the Contractor fails to perform any of the provisions of this contract, or
- the Contractor fails to make progress as to endanger performance of this contract in accordance with its terms.

The Director of Purchases shall provide Contractor with written notice of the conditions endangering performance. If the Contractor fails to remedy the conditions within ten (10) days from the receipt of the notice (or such longer period as State may authorize in writing), the Director of Purchases shall issue the Contractor an order to stop work immediately. Receipt of the notice shall be presumed to have occurred within three (3) days of the date of the notice.

### 3.11. Termination for Convenience

The Director of Purchases may terminate performance of work under this contract in whole or in part whenever, for any reason, the Director of Purchases shall determine that the termination is in the best interest of the State of Kansas. In the event that the Director of Purchases elects to terminate this contract pursuant to this provision, it shall provide the Contractor written notice at least 30 days prior to the termination date. The termination shall be effective as of the date specified in the notice. The Contractor shall continue to perform any part of the work that may have not been terminated by the notice.

### 3.12. Rights and Remedies

If this contract is terminated, the State, in addition to any other rights provided for in this contract, may require the Contractor to transfer title and deliver to the State in the manner and to the extent directed, any completed materials. The State shall be obligated only for those services and materials rendered and accepted prior to the date of termination.

In the event of termination, the Contractor shall receive payment prorated for that portion of the contract period services were provided to or goods were accepted by State subject to any offset by State for actual damages including loss of federal matching funds.

The rights and remedies of the State provided for in this contract shall not be exclusive and are in addition to any other rights and remedies provided by law.

### 3.13. Debarment of State Contractors

Any Contractor who defaults on delivery or does not perform in a satisfactory manner as defined in this Contract may be barred for a period up to three (3) years, pursuant to KSA 75-37,103, or have their work evaluated for pre-qualification purposes pursuant to K.S.A. 75-37,104.

### 3.14. Antitrust

If the Contractor elects not to proceed with performance under any such contract with the State, the Contractor assigns to the State all rights to and interests in any cause of action it has or may acquire under the anti-trust laws of the United States and the State of Kansas relating to the particular products or services purchased or acquired by the State pursuant to this contract.

### 3.15. Breach

Waiver or any breach of any contract term or condition shall not be deemed a waiver of any prior or subsequent breach. No contract term or condition shall be held to be waived, modified, or deleted except by a written instrument signed by the parties thereto.

If any contract term or condition or application thereof to any person(s) or circumstances is held invalid, such invalidity shall not affect other terms, conditions, or applications which can be given effect without the invalid term, condition or application. To this end the contract terms and conditions are severable.

### 3.16. Hold Harmless

The Contractor shall indemnify the State against any and all loss or damage to the extent arising out of the Contractor's negligence in the performance of services under this contract and for infringement of any copyright or patent occurring in connection with or in any way incidental to or arising out of the occupancy, use, service, operations or performance of work under this contract.

The State shall not be precluded from receiving the benefits of any insurance the Contractor may carry which provides for indemnification for any loss or damage to property in the Contractor's custody and control, where such loss or destruction is to state property. The Contractor shall do nothing to prejudice the State's right to recover against third parties for any loss, destruction or damage to State property.

### 3.17. Force Majeure

The Contractor shall not be held liable if the failure to perform under this contract arises out of causes beyond the control of the Contractor. Causes may include, but are not limited to, acts of nature, fires, tornadoes, quarantine, strikes other than by Contractor's employees, and freight embargoes.

### 3.18. Assignment

The Contractor shall not assign, convey, encumber, or otherwise transfer its rights or duties under this contract without the prior written consent of the State. State may reasonably withhold consent for any reason.

This contract may terminate for cause in the event of its assignment, conveyance, encumbrance or other transfer by the Contractor without the prior written consent of the State.

### 3.19. Third Party Beneficiaries

This contract shall not be construed as providing an enforceable right to any third party.

### 3.20. Waiver

Waiver of any breach of any provision in this contract shall not be a waiver of any prior or subsequent breach. Any waiver shall be in writing and any forbearance or indulgence in any other form or manner by State shall not constitute a waiver.

### 3.21. Injunctions

Should Kansas be prevented or enjoined from proceeding with the acquisition before or after contract execution by reason of any litigation or other reason beyond the control of the State, Contractor shall not be entitled to make or assert claim for damage by reason of said delay.

### 3.22. Staff Qualifications

The Contractor shall warrant that all persons assigned by it to the performance of this contract shall be employees of the Contractor (or specified Subcontractor) and shall be fully qualified to perform the work required. The Contractor shall include a similar provision in any contract with any Subcontractor selected to perform work under this contract.

Failure of the Contractor to provide qualified staffing at the level required by the contract specifications may result in termination of this contract or damages.

### 3.23. Subcontractors

The Contractor shall be the sole source of contact for the contract. The State will not subcontract any work under the contract to any other firm and will not deal with any subcontractors. The Contractor is totally responsible for all actions and work performed by its subcontractors. All terms, conditions and requirements of the contract shall apply without qualification to any services performed or goods provided by any subcontractor.

### 3.24. Independent Contractor

Both parties, in the performance of this contract, shall be acting in their individual capacity and not as agents, employees, partners, joint ventures or associates of one another. The employees or agents of one party shall not be construed to be the employees or agents of the other party for any purpose whatsoever.

The Contractor accepts full responsibility for payment of unemployment insurance, workers compensation, social security, income tax deductions and any other taxes or payroll deductions required by law for its employees engaged in work authorized by this contract.

### 3.25. Worker Misclassification

The Contractor and all lower tiered subcontractors under the Contractor shall properly classify workers as employees rather than independent contractors and treat them accordingly for purposes of workers' compensation insurance coverage, unemployment taxes, social security taxes, and income tax withholding. Failure to do so may result in contract termination.

### 3.26. Immigration and Reform Control Act of 1986 (IRCA)

All contractors are expected to comply with the Immigration and Reform Control Act of 1986 (IRCA), as may be amended from time to time. This Act, with certain limitations, requires the verification of the employment status of all individuals who were hired on or after November 6, 1986, by the Contractor as well as any subcontractor or sub-contractors. The usual method of verification is through the Employment Verification (I-9) Form.

With the submission of this bid, the Contractor hereby certifies without exception that such Contractor has complied with all federal and state laws relating to immigration and reform. Any misrepresentation in this regard or any employment of persons not authorized to work in the United States constitutes a material breach and, at the State's option, may subject the contract to termination for cause and any applicable damages.

Unless provided otherwise herein, all contractors are expected to be able to produce for the State any documentation or other such evidence to verify Contractor's IRCA compliance with any provision, duty, certification or like item under the contract.

Contractor will provide a copy of a signed Certification Regarding Immigration Reform and Control Form (http://admin.ks.gov/docs/default-source/ofpm/procurement-contracts/irca.doc?sfvrsn=6) with the technical proposal.

### 3.27. Proof of Insurance

Upon request, the Contractor shall present an affidavit of Worker's Compensation, Public Liability, and Property Damage Insurance to Procurement and Contracts.

### 3.28. Conflict of Interest

The Contractor shall not knowingly employ, during the period of this contract or any extensions to it, any professional personnel who are also in the employ of the State and providing services involving this contract or services similar in nature to the scope of this contract to the State. Furthermore, the Contractor shall not knowingly employ, during the period of this contract or any extensions to it, any state employee who has participated in the making of this contract until at least two years after his/her termination of employment with the State.

### 3.29. Nondiscrimination and Workplace Safety

The Contractor agrees to abide by all federal, state and local laws, and rules and regulations prohibiting discrimination in employment and controlling workplace safety. Any violations of applicable laws or rules or regulations may result in termination of this contract.

### 3.30. Confidentiality

The Contractor may have access to private or confidential data maintained by State to the extent necessary to carry out its responsibilities under this contract. Contractor must comply with all the requirements of the Kansas Open Records Act (K.S.A. 45-215 et seq.) in providing services under this contract. Contractor shall accept full responsibility for providing adequate supervision and training to its agents and employees to ensure compliance with the Act. No private or confidential data collected, maintained or used in the course of performance of this contract shall be disseminated by either party except as authorized by statute, either during the period of the contract or thereafter. Contractor agrees to return any or all data furnished by the State promptly at the request of State in whatever form it is maintained by Contractor. On the termination or expiration of this contract, Contractor shall not use any of such data or any material derived from the data for any purpose and, where so instructed by State, shall destroy or render it unreadable.

### 3.31. Environmental Protection

The Contractor shall abide by all federal, state and local laws, and rules and regulations regarding the protection of the environment. The Contractor shall report any violations to the applicable governmental agency. A violation of applicable laws or rule or regulations may result in termination of this contract for cause.

### 3.32. Care of State Property

The Contractor shall be responsible for the proper care and custody of any state owned personal tangible property and real property furnished for Contractor's use in connection with the performance of this contract. The Contractor shall reimburse the State for such property's loss or damage caused by the Contractor, except for normal wear and tear.

### 3.33. Prohibition of Gratuities

Neither the Contractor nor any person, firm or corporation employed by the Contractor in the performance of this contract shall offer or give any gift, money or anything of value or any promise for future reward or compensation to any State employee at any time.

### 3.34. Retention of Records

Unless the State specifies in writing a different period of time, the Contractor agrees to preserve and make available at reasonable times all of its books, documents, papers, records and other evidence involving transactions related to this contract for a period of five (5) years from the date of the expiration or termination of this contract.

Matters involving litigation shall be kept for one (1) year following the termination of litigation, including all appeals, if the litigation exceeds five (5) years.

The Contractor agrees that authorized federal and state representatives, including but not limited to, personnel of the using agency; independent auditors acting on behalf of state and/or federal agencies shall have access to and the right to examine records during the contract period and during the five (5) year post contract period. Delivery of and access to the records shall be within five (5) business days at no cost to the state.

### 3.35. Off-Shore Sourcing

If, during the term of the contract, the Contractor or subcontractor plans to move work previously performed in the United States to a location outside of the United States, the Contractor shall immediately notify the Procurement and Contracts and the respective agency in writing, indicating the desired new location, the nature of the work to be moved and the percentage of work that would be relocated. The Director of Purchases, with the advice of the respective agency, must approve any changes prior to work being relocated. Failure to obtain the Director's approval may be grounds to terminate the contract for cause.

### 3.36. On-Site Inspection

Failure to adequately inspect the premises shall not relieve the Contractor from furnishing without additional cost to the State any materials, equipment, supplies or labor that may be required to carry out the intent of this Contract.

### 3.37. Indefinite Quantity Contract

This is an open-ended contract between the Contractor and the State to furnish an undetermined quantity of a good or service in a given period of time. The quantities ordered will be those actually required during the contract period, and the Contractor will deliver only such quantities as may be ordered. No guarantee of volume is made. An estimated quantity based on past history or other means may be used as a guide.

### 3.38. Prices

Prices shall remain firm for the entire contract period and subsequent renewals. Prices shall be net delivered, including all trade, quantity and cash discounts. Any price reductions available during the contract period shall be offered to the State of Kansas. Failure to provide available price reductions may result in termination of the contract for cause.

### 3.39. Payment

Payment Terms are Net 30 days. Payment date and receipt of order date shall be based upon K.S.A. 75-6403(b). This Statute requires state agencies to pay the full amount due for goods or services on or before the 30th calendar day after the date the agency receives such goods or services or the bill for the goods and services, whichever is later, unless other provisions for payment are agreed to in writing by the Contractor and the state agency. NOTE: If the 30th calendar day noted above falls on a Saturday, Sunday, or legal holiday, the following workday will become the required payment date.

Payments shall not be made for costs or items not listed in this contract.

Payment schedule shall be on a frequency mutually agreed upon by both the agency and the Contractor.

### 3.40. Invoices

Each purchase order must be individually invoiced. Invoices shall be forwarded to the using agency in duplicate and shall state the following:

- date of invoice.
- date of shipment (or completion of work);
- purchase order number and contract number;
- itemization of all applicable charges; and
- net amount due.

### 3.41. Accounts Receivable Set-Off Program

If, during the course of this contract the Contractor is found to owe a debt to the State of Kansas, agency payments to the Contractor may be intercepted / setoff by the State of Kansas. Notice of the setoff action will be provided to the Contractor. Pursuant to K.S.A. 75-6201 et seq, Contractor shall have the opportunity to challenge the validity of the debt. If the debt is undisputed, the Contractor shall credit the account of the agency making the payment in an amount equal to the funds intercepted.

K.S.A. 75-6201 et seq. allows the Director of Accounts & Reports to setoff funds the State of Kansas owes Contractors against debts owed by the Contractors to the State of Kansas. Payments setoff in this manner constitute lawful payment for services or goods received. The Contractor benefits fully from the payment because its obligation to the State is reduced by the amount subject to setoff.

### 3.42. Federal, State and Local Taxes

Unless otherwise specified, the contracted price shall include all applicable federal, state and local taxes. The Contractor shall pay all taxes lawfully imposed on it with respect to any product or service delivered in accordance with this Contract. The State of Kansas is exempt from state sales or use taxes and federal excise taxes for direct purchases. These taxes shall not be included in the contracted price. Upon request, the State shall provide to the Contractor a certificate of tax exemption.

The State makes no representation as to the exemption from liability of any tax imposed by any governmental entity on the Contractor.

### 3.43. Shipping and F.O.B. Point

Unless otherwise specified, prices shall be F.O.B. DESTINATION, PREPAID AND ALLOWED (included in the price bid), which means delivered to a state agency's receiving dock or other designated point as specified in this contract or subsequent purchase orders without additional charge. Shipments shall be made in order to arrive at the destination at a satisfactory time for unloading during receiving hours.

### 3.44. Deliveries

All orders shall be shipped within a to be determined number of days ARO, clearly marked with the purchase order number. If delays in delivery are anticipated, the Contractor shall immediately notify the ordering agency of the revised delivery date or partial delivery date. The order may be canceled if delivery time is unsatisfactory. The Contractor shall inform Procurement and Contracts of any supply or delivery problems. Continued delivery problems may result in termination of the contract for cause.

### 3.45. Charge Back Clause

If the Contractor fails to deliver the product within the delivery time established by the contract, the State reserves the right to purchase the product from the open market and charge back the difference between contract price and open market price to the Contractor.

### 3.46. Debarment of State Contractors

Any Contractor who defaults on delivery or does not perform in a satisfactory manner as defined in this Agreement may be barred for up to a period of three (3) years, pursuant to K.S.A. 75-37,103, or have its work evaluated for pre-qualification purposes. Contractor shall disclose any conviction or judgment for a criminal or civil offense of any employee, individual or entity which controls a company or organization or will perform work under this Agreement that indicates a lack of business integrity or business honesty. This includes (1) conviction of a criminal offense as an incident to obtaining or attempting to obtain a public or private contract or subcontract or in the performance of such contract or subcontract; (2) conviction under state or federal statutes of embezzlement, theft, forgery, bribery, falsification or destruction of records, receiving stolen property; (3) conviction under state or federal antitrust statutes; and (4) any other offense to be so serious and compelling as to affect responsibility as a state contractor. For the purpose of this section, an individual or entity shall be presumed to have control of a company or organization if the individual or entity directly or indirectly, or acting in concert with one or more individuals or entities, owns or controls 25 percent or more of its equity, or otherwise controls its management or policies. Failure to disclose an offense may result in the termination of the contract.

### 3.47. Materials and Workmanship

The Contractor shall perform all work and furnish all supplies and materials, machinery, equipment, facilities, and means, necessary to complete all the work required by this Contract, within the time specified, in accordance with the provisions as specified.

The Contractor shall be responsible for all work put in under these specifications and shall make good, repair and/or replace, at the Contractor's own expense, as may be necessary, any defective work, material, etc., if in the opinion of agency and/or Procurement and Contracts said issue is due to imperfection in material, design, workmanship or Contractor fault.

**3.48. Industry Standards**

If not otherwise provided, materials or work called for in this contract shall be furnished and performed in accordance with best established practice and standards recognized by the contracted industry and comply with all codes and regulations which shall apply.

**3.49. Implied Requirements**

All products and services not specifically mentioned in this contract, but which are necessary to provide the functional capabilities described by the specifications, shall be included.

**3.50. Submission of the Bid**

Submission of the bid will be considered presumptive evidence that the bidder is conversant with local facilities and difficulties, the requirements of the documents and of pertinent State and/or local codes, state of labor and material markets, and has made due allowances in the proposal for all contingencies. Later claims for labor, work, materials, equipment, and tax liability required for any difficulties encountered which could have been foreseen will not be recognized and all such difficulties shall be properly taken care of by Contractor at no additional cost to the State of Kansas.

**3.51. New Materials, Supplies or Equipment**

Unless otherwise specified, all materials, supplies or equipment offered by the Contractor shall be new, unused in any regard and of most current design. All materials, supplies and equipment shall be first class in all respects. Seconds or flawed items will not be acceptable. All materials, supplies or equipment shall be suitable for their intended purpose and, unless otherwise specified, fully assembled and ready for use on delivery

**3.52. Warranty**

Bidders shall indicate the type and extent of the warranty for all products, equipment, hardware, software, and services proposed. The State requires a "standard" warranty of a specific amount of days, or one year, whichever is greater. This warranty shall be included in the cost of the product, equipment, hardware, software, and services proposed.

The Contractor warrants that it is either the sole owner of all right, title and interest in and to, or is authorized to license to the state the Software being provided under this contract. The Contractor will be the sole point of contact on any problems with the product, equipment or systems during the warranty period.

**3.53. Inspection**

The State reserves the right to reject, on arrival at destination, any items which do not conform with specification of the Contract.

**3.54. Acceptance**

No contract provision or use of items by the State shall constitute acceptance or relieve the Contractor of liability in respect to any expressed or implied warranties.

**3.55. Ownership**

All data, forms, procedures, software, manuals, system descriptions and work flows developed or accumulated by the Contractor under this contract shall be owned by the using agency. The Contractor may not release any materials without the written approval of the using agency.

**3.56. Information/Data**

Any and all information/data required to be provided at any time during the contract term shall be made available in a format as requested and/or approved by the State.

**3.57. Certification of Materials Submitted**

The Bid document, together with the specifications set forth herein and all data submitted by the Contractor to support their response including brochures, manuals, and descriptions covering the operating characteristics of the item(s) proposed, shall become a part of the contract between the Contractor and the State of Kansas. Any written representation

covering such matters as reliability of the item(s), the experience of other users, or warranties of performance shall be incorporated by reference into the contract.

**3.58. Transition Assistance**

In the event of contract termination or expiration, Contractor shall provide all reasonable and necessary assistance to State to allow for a functional transition to another vendor.

**3.59. Integration**

This contract, in its final composite form, shall represent the entire agreement between the parties and shall supersede all prior negotiations, representations or agreements, either written or oral, between the parties relating to the subject matter hereof. This Agreement between the parties shall be independent of and have no effect on any other contracts of either party.

**3.60. Modification**

This contract shall be modified only by the written agreement and approval of the parties. No alteration or variation of the terms and conditions of the contract shall be valid unless made in writing and signed by the parties. Every amendment shall specify the date on which its provisions shall be effective.

**3.61. Severability**

If any provision of this contract is determined by a court of competent jurisdiction to be invalid or unenforceable to any extent, the remainder of this contract shall not be affected and each provision of this contract shall be enforced to the fullest extent permitted by law.

**3.62. Software Code and Intellectual Property Rights**

As applicable, all original software and software code and related intellectual property developed or created by the Contractor in the performance of its obligations under this Contract or any Task Order issued under this Contract, shall become the sole property of the State of Kansas. The Contractor will surrender all original written materials, including any reports, studies, designs, drawings, specifications, notes, documents, software and documentation, computer-based training modules, electronically or magnetically recorded material, used to develop this software or software code and related intellectual property to the state entity for which it was developed
If Contractor is relying upon a copyrighted work to fulfill the specifications required in this contract, then the state agrees to keep the copyrighted work in confidence and to take all reasonable precautions to ensure that no unauthorized persons have access to the copyrighted work or to documentation that may contain proprietary intellectual property rights.

Vendor must submit the copyrighted documents to be considered as Trade secrets or proprietary information and legally recognized as such and protected by law, if clearly labeled "Proprietary" on each individual page and provided as separate from the main proposal. Pricing information is not considered proprietary and the bidder's entire proposal response package will not be considered proprietary.

All information requested to be handled as "Proprietary" shall be submitted separately from the main proposal and clearly labeled, in a separate envelope or clipped apart from all other documentation. The bidder shall provide detailed written documentation justifying why this material should be considered "Proprietary". The Office of Procurement and Contracts reserves the right to accept, amend or deny such requests for maintaining information as proprietary in accordance with Kansas law.

**3.63. Escrow of Software Source Materials**

Contractor shall provide for the escrow, in Topeka, Kansas, of a currently operating copy of the proprietary software source code and standard documentation in escrow. Within 20 days after the state accepts the software being developed pursuant to this contract, the Contractor shall deliver a sealed package to the Escrow Agent previously agreed to by the parties. The package containing the source code and relevant standard documentation for the software purchased under this contract shall be deposited with the Escrow Agent for safekeeping. The Escrow Agent shall notify the contractor in writing of receipt of the package and shall certify that the seal was unbroken. As the contractor subsequently sends sealed packages containing updates, changes, or modifications to the software, the Escrow Agent shall likewise certify their arrival with seals intact and shall, within 10 days, return prior packages in a sealed condition. Any modification, updates, new releases, or documentation related to the source code copy shall be deposited with the Escrow Agency as soon as practicable after any software release, but not longer than 30 days after release.

The package containing the source code and documentation shall not be opened nor its seal broken unless: (a) the contractor notifies the state in writing to permit breaking the seal; (b) the contractor ceases doing business and the

business is not continued by another entity; and (c) the contractor becomes unable, or otherwise fails in material respect to support the systems, as required by written contract between the parties, or to maintain the systems as provided in this contract. Breaking the seal of any package held pursuant to this contract shall be only for the limited purposes of supporting and maintaining the software in use in the courts of the state of Kansas and for no other purposes. If the contract between the parties is terminated for any reason other than a reason listed in this provision, the source code package shall be immediately returned to the contractor.

**3.64. Award**

Award will be by line item or group total, whichever is in the best interest of the State of Kansas.

## 4. SPECIFICATIONS

### 4.1. Scope of Work

The Preparedness program within the Bureau of Community Health Systems (BCHS) at the Kansas Department of Health and Environment (KDHE) provides leadership to protect the health of Kansans through efforts to mitigate, prepare for, respond to, and recover from disasters, infectious disease, terrorism, and mass casualty emergencies. To accomplish this mission, the Preparedness program is responsible for the following:

- Health and medical planning and response in Kansas
- Serves as the coordinating unit for the Emergency Support Function (ESF) #8
- Maintains the Health Alert Network (KS-HAN)
- Serves as the grantee for the Centers for Disease Control and Prevention (CDC) and Health and Human services (HHS) health preparedness grants

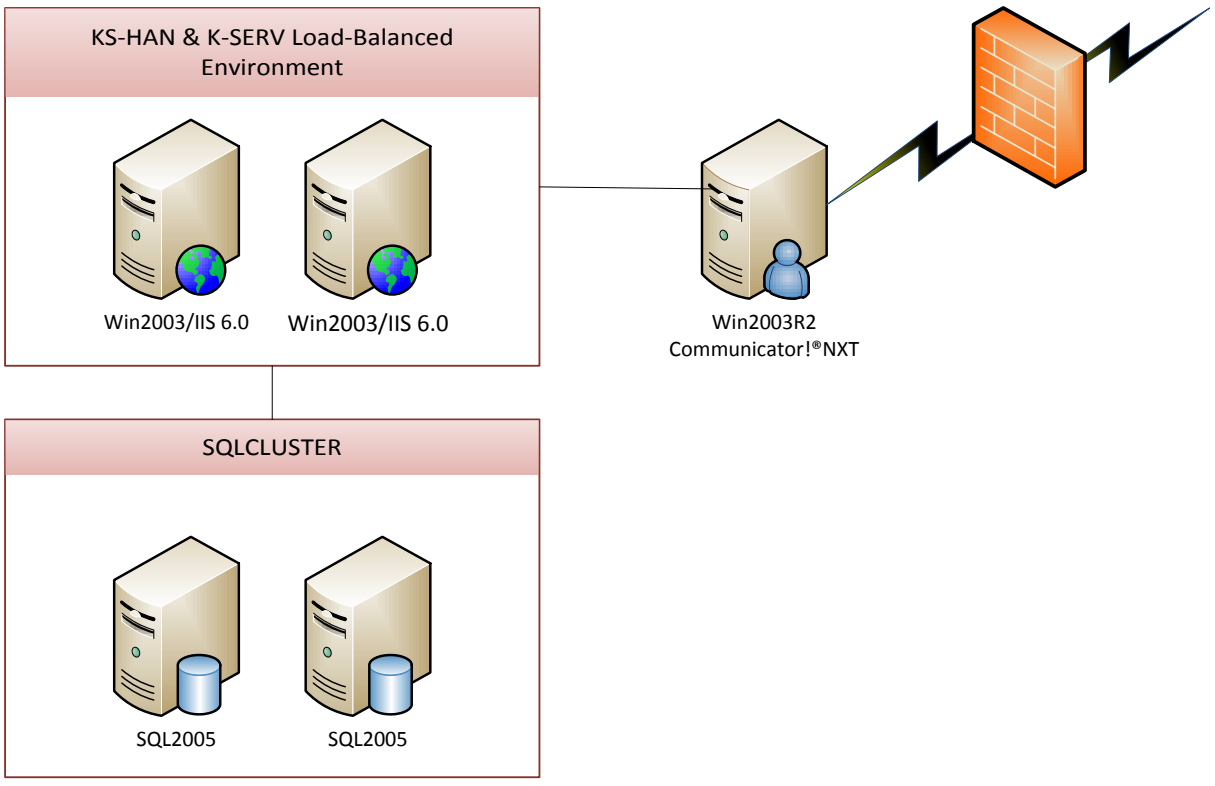
To assist and support preparedness efforts, the Preparedness program hosts four (4) information technologysystems; two of these systems are the Kansas Health Alert Network (KS-HAN) and the Kansas System for the Early Registration of Volunteers (K-SERV).

KS-HAN is a secure, web-based notification system that enables local and state emergency health and safety entities to share public and environmental health and general emergency preparedness information rapidly. The system allows users to send, receive and discuss information in a secure environment. Additionally, KS-HAN can be utilized as a document storing and sharing website. It also allows for the rapid notification of any and all users in the event of an emergency, when the timely distribution of recommendations on investigation, prevention and treatment is critical. KS-HAN has the ability to alert registrants by organization, occupation, county, or group through e-mail, work and cell phone, and SMS text. KS-HAN is an invitation-only registration system with over 4000 participants, who represent local health departments, hospitals, emergency management and many other critical first responder agencies across the state.

K-SERV is a secure registration system and database for volunteers willing to respond to public health emergencies or other disasters in Kansas or other areas across the country. It can be utilized as a volunteer management system at the local and state levels, therefore avoiding duplication of information at each level. Everyone is welcome to register in K-SERV. K-SERV is based on the standards developed by the federal Emergency System for the Advance Registration of Volunteer Health Professionals (ESAR-VHP) program. By registering through K-SERV, volunteers' identities, licenses, credentials, accreditations, and hospital privileges are all verified in advance, saving valuable time in emergency situations.

The KS-HAN and K-SERV hardware and software platforms (Microsoft Windows® 2003/Internet Information Services (IIS) 6.0, SQL Server 2005) are outdated and in need of upgrading. Both KS-HAN and K-SERV systems were developed in-house using a .Net 4.0 framework with web controls that are now out-of-support. As the diagram illustrates below, the applications run on two load-balanced servers that share the same SQL® database cluster. KS-HAN currently utilizes the Cassidian (now known as Airbus DS Communications) "Communicator!®NXT" v4.2.1 product for mass notifications. Kansas limits the mass notification environment to 15 concurrent users due to license cost per concurrent user; this concurrent-user license constraint causes potential issues during an emergency health situation utilizing the alert system.

The Kansas Department of Health and Environment (KDHE) is requesting proposals from vendors for a system to replace the registration, user management, reporting, and messaging components of the Kansas Health Alert Network (KS-HAN) and Kansas System for the Early Registration of Volunteers (K-SERV) Systems. KDHE would like to procure new software for this system that will provide greater functionality and flexibility for users and recipients. The requirements for this new system are detailed in APPENDIX B: Requirements Table of this Request for Proposal.




Current KS-HAN & K-SERV Environment Diagram

**ACRONYMS**

| Acronym | Definition |
|---|---|
| BCHS | Bureau of Community Health Services |
| ESAR-VHP | Emergency System for the Advance Registration of Volunteer Health Professionals |
| ITEC | Information Technology Executive Council |
| KDHE | Kansas Department of Health and Environment |
| K-SERV | Kansas System for the Early Registration of Volunteers |
| KS-HAN | Kansas Health Alert Network |

### 4.2. Requirements

1. **State and Federal Debarment Suspension Certification**:
   The vendor shall have knowledge of and shall comply with the following State and Federal requirements:
   1.1. State and Federal Debarment Suspension Certification, Appendix A of 49 CFR 29.510.
   1.2. The bidder is advised that Appendix A of 49 CFR 29.510 requires that the bidder, including all principals representing the organization, certify that they are not currently under debarment or suspension or have not been under debarment or suspension within the past three years. (Refer to certification instructions in this document's **APPENDIX A**).
2. **Confidentiality**:
   Vendor will have access to Confidential Information and private or confidential data maintained by the State, to the extent necessary to carry out Vendor's responsibilities. Vendor agrees that all Confidential Information shall be and shall remain the sole property of the State and Vendor holds any such Confidential Information in trust and confidence for the State. This Confidential Information and data includes personal identifiable information. Vendor also agrees to the following:
   2.1. All the information and data (including individual or other information identified by the State) of the State shall be considered confidential and private. All electronic data shall be secured through encryption or other comparable security measure.
   2.2. Vendor agrees that it and its employees will not, during the performance of or after the termination of this Agreement, disseminate or disclose at any time to any person, firm, corporation, or other entity, or use for its own business or benefit any information or data (including but not limited to use of names, home addresses, phone numbers of employees or citizens; or any other information obtained about employees, citizens, or vendors) obtained by it while in the performance of this Agreement.
   2.3. Vendor shall not remove Confidential Information from State's site without State's prior written approval. Notwithstanding the foregoing, email and similar communications contained on Vendor laptops shall not be considered Confidential Information and approval is granted, subject to compliance with applicable security policies, for Vendor laptops to be removed from the State's site.
   2.4. Vendor shall limit access to Confidential Information solely to Vendor staff that has a business need to know for purposes of fulfilling Vendor's obligations under this Agreement. Any staff, individual or entity assigned to work for Vendor under this Agreement shall separately sign a *Vendor Employee Computer and Network User Agreement* and be bound by the requirements of this Article. See **APPENDIX D** for *Vendor Employee Computer and Network User Agreement.*
   2.5. Vendor agrees to comply and shall be fully responsible for providing adequate supervision and training to its agents and employees to ensure Vendor's (and subcontractors of Vendor) compliance with all applicable State and Federal Acts regarding confidentiality and the Kansas Open Records Act, K.S.A. 45-215 *et seq*.
   2.6. Upon termination or expiration of this Agreement, or at the State's request, Vendor and each of the persons and entities working for the Vendor, including any subcontractors, shall promptly destroy or return to the State all Confidential Information, including all data, information electronic, written, or descriptive materials or any related matter of any type, including but not limited to drawings, blueprints, descriptions, or other papers or documents which contain any such Confidential Information and shall not make, retain or distribute any copies thereof.
   2.7. The State will ensure that Vendor's properly marked and designated "confidential information", or information that should by its nature be obviously understood to be confidential, including without limitation social security numbers and personal private information, is not disclosed to others except as required by the Kansas Open Records Act. Vendor acknowledges and agrees that the State may be required to disclose certain information of Vendor pursuant to the Kansas Open Records Act.
   2.8. Vendor shall develop and maintain a security plan for the Project pursuant to its internal Client Data Protection Policies. Such plan shall be subject to review and approval by the State. Upon approval, Vendor shall implement and comply with such plan to secure and protect all personal and private information or personal health information. Vendor shall hold State harmless and indemnify the State for expenses or damages, of any kind, incurred or suffered by the State as a result of any failure by Vendor to comply with such plan. Vendor shall notify the State of any loss or breach of confidential information or data within twenty-four (24) hours of such knowledge. Vendor shall also be responsible and liable for any and all damages to individuals due to such breaches. In the event of any failure to comply with the security plan in which the Confidential Information of one or more individuals is lost, compromised, or is potentially compromised, Vendor shall be responsible and pay for any and all damages, expenses, and costs (including but not limited to lost wages and efforts spent to defend or

correct against identity theft) caused to the State or any individual for the disclosure of any Confidential Information. In the event of such breach, Vendor shall provide notice to the State and affected individuals of such disclosure and shall also offer free of charge to affected individuals and the State, identity theft protection insurance for a period of up to two (2) years up to an aggregate cap of one million dollars ($1,000,000). Such identity theft protection insurance shall be the sole and exclusive remedy against Vendor with respect to a breach under this provision. These terms shall also apply to any third-party vendors or subcontractors.

**3. Fixed Costs Final and Full:**

3.1. All reasonable and necessary equipment, labor, software, and services to make this Project timely operational shall be included in the proposal and included in the fixed costs. The Vendor is responsible for all additional costs not included in the proposal and required to satisfactorily complete the scope of services requested and the State's requirements.

3.2. This Request is for a firm fixed price contract with payment(s) made only for defined and accepted deliverables.

3.3. Prices shall remain firm for the entire contract period and subsequent renewals. Prices quoted shall be net delivered, including all trade, quantity, and cash discounts.

3.4. Any price reductions available during the contract period shall be offered to the State of Kansas.

3.5. Failure to provide available price reductions may result in termination of the contract.

3.6. The State will not award or contract for any arrangement that uses estimates, "time and materials," or payments based on "progress" or elapsed time.

3.7. The exact payment per deliverable will be determined during negotiations.

**4. Independent Vendor:**

4.1. Both parties, in the performance of this contract, shall be acting in their individual capacity and not as agents, employees, partners, joint ventures or associates of one another. The employees or agents of one party shall not be construed to be the employees or agents of the other party for any purpose whatsoever.

4.2. The Vendor accepts full responsibility for payment of unemployment insurance, workers compensation and social security as well as all income tax deductions and any other taxes or payroll deductions required by law for its employees engaged in work authorized by this contract.

**5. Subcontractors:**

5.1. The Vendor shall be the sole source of contact for the contract. The State will not subcontract any work under the contract to any other firm and will not deal with any subcontractors. The Vendor is totally responsible for all actions and work performed by its subcontractors. All terms, conditions and requirements of the contract shall apply without qualification to any services performed or goods provided by any subcontractor.

**6. Federal, State and Local Taxes:**

6.1. Unless otherwise specified, the proposal price shall include all applicable federal, state and local taxes. The successful vendor shall pay all taxes lawfully imposed on it with respect to any product or service delivered in accordance with this Request. **The State of Kansas is exempt from state sales or use taxes and federal excise taxes for direct purchases. These taxes shall not be included in the vendor's price quotation.**

6.2. The State makes no representation as to the exemption from liability of any tax imposed by any governmental entity on the Vendor.

**7. Demonstration Requirements:**

7.1. A demonstration of the selected devices/equipment/solution for the using agencies may be required before final contract approval. The State of Kansas reserves the right to request said devices/equipment/solution fully configured/operational for testing, which shall be furnished at no expense to the State within ten (10) days after receipt of request. Devices/equipment will be returned at the bidder's expense if found to be non-compliant with the specifications as set forth in this proposal.

**8. Implied Requirements:**

8.1. All products and services not specifically mentioned in this solicitation, but which are necessary to provide the functional capabilities described by the specifications, shall be included. Furthermore, all products and services required to make the vendor's proposal functional shall be identified in the vendor's proposal. If additional products or services are later found to be necessary to make the vendor's proposal functional, or to make the

vendor's proposal compliant with the specifications, regardless of whether the additional needed products or services are identified as being necessary by the State or the vendor, such products or services shall be provided by the vendor at no charge to the State.

**9. Warranty:**

9.1. Bidders shall indicate the type and extent of the warranty for all equipment, hardware, software, and services proposed. The State requires a "standard" warranty of a specific amount of days, or 1 year, whichever is greater. This warranty shall be included in the cost of the equipment.

9.2. The successful bidder will be the sole point of contact on any problems with the equipment or systems during the warranty period.

9.3. The Vendor shall be responsible for all work performed under these specifications. The Vendor shall make good, repair and replace, at the Vendor's own expense, as may be necessary, any defective work, material acceptance, if in the opinion of agency and/or Division of Purchases said defect is due to imperfection in material, design, or workmanship for the warranty period specified.

**10. Ownership:**

10.1. All data, forms, procedures, software, manuals, system descriptions and work flows developed or accumulated by the Vendor under this contract shall be owned by the using agency. The Vendor may not release any materials without the written approval of the using agency.

**11. Certification of Materials Submitted:**

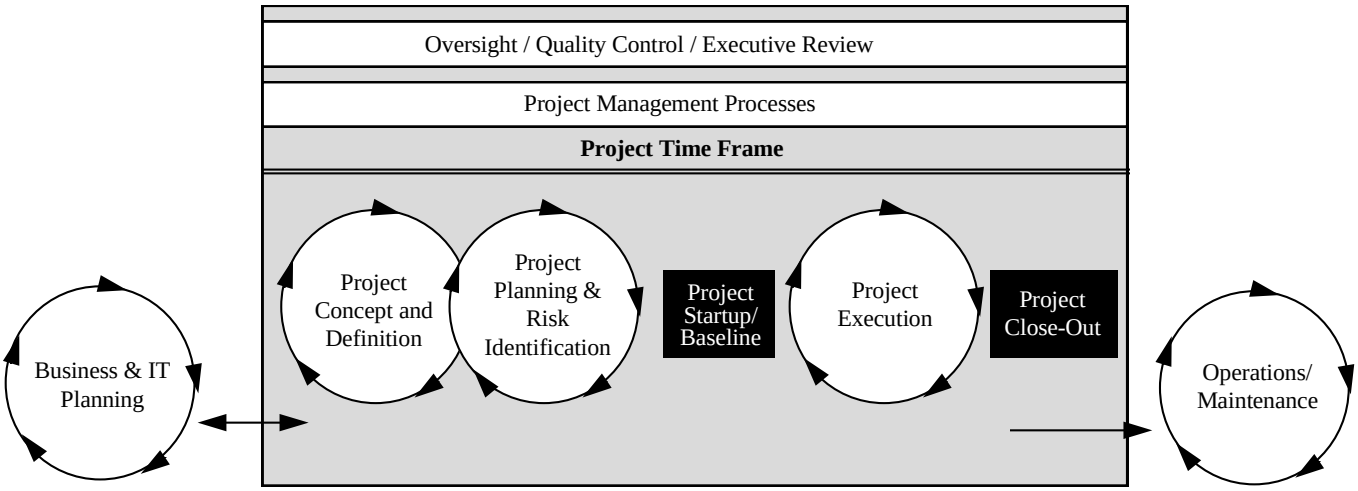
11.1. The response to this request, together with the specifications set forth herein and all data submitted by the vendor to support the response including brochures, manuals, and descriptions covering the operating characteristics of the item(s) proposed, shall become a part of any contract between the successful vendor and the State of Kansas. Any written representation covering such matters as reliability of the item(s), the experience of other users, or warranties of performance shall be incorporated by reference into the contract.

**12. V**endor Contracts:

12.1. Include a copy of any contracts, agreements, licenses, warranties, etc. proposed. (State of Kansas form DA-146a remains a mandatory requirement in all contracts.)

**13. Vendor Project Coordinator:**

13.1. Vendor must provide qualified staff to assist the KDHE project manager during solution implementation. This vendor resource must be able to develop and understand the **D1. *Detailed Project Plan*** deliverable found in Section 6 and participate in project status briefings. Kansas information technology projects follow the Kansas Information Technology Executive Council (ITEC) Project Management Methodology outlined in Figure 1 below. Additional information concerning this methodology may be found at https://oits.ks.gov/kito/kito-home .




**14. Specific Solution Requirements:**

14.1 Requirements not listed above are included in **APPENDIX B**: *Requirements Table*. This Table refers to basic functional, geospatial, security, hosting, reporting, and other technical requirements needed in the proposed solution. Vendor is expected to return this completed table as part of the technical response.

### 4.3. Services to be Provided

**1. SOFTWARE AS A SERVICE (SAAS):**

Vendor is responsible for deployment of solution as a hosted service. KDHE approved end users will access proposed solution over the Internet. Vendor will host proposed solution and KDHE data centrally, deploying patches and enhancements transparently and delivering access to KDHE approved end users over the Internet. Vendor SAAS responsibilities include:

1.1. Providing KDHE hosting and access services related to the proposed application through the web, permitting data entry by KDHE and providing information management for KDHE.
1.2. Providing all infrastructures needed for production, test and disaster recovery environments.
1.3. Ensuring access to the application twenty-four (24) hours a day seven (7) days a week.
1.4. Collaborating with other KDHE Vendors and/or partners as needed.
1.5. Performing test and installation of patches.
1.6. Managing enhancements.
1.7. Monitoring performance.
1.8. Applying best practices to enhance program integration.

2. **HELPDESK AND INCIDENT MANAGEMENT SERVICES**:

2.1. **System Performance Services:** Vendor is responsible for system performance as it pertains to hardware and network configuration issues. Vendor is responsible for performance as it relates to software and database programming, including on-going system maintenance needs and database tuning. Specific metrics, producible in a controlled environment, include:

2.1.1. Monthly uptime percentage shall be 98.9% except for downtime agreed upon by the Vendor and KDHE for system maintenance and enhancements.

2.2. **HelpDesk Services:** KDHE agrees to provide a Level 1 user help desk. Vendor agrees to provide Level 2 and Level 3 technical support.

2.2.1. Level 1 (L1): Provided by KDHE. Document issues identified by users.
2.2.2. Level 2 (L2): Provided by Vendor. Application usage, technical support, minor to intermediate host fixes, minor code fixes, workarounds, test and package large issues for L3.
2.2.3. Level 3 (L3): Provided by Vendor. Involves code fixes.

2.3. **Incident Management Services:** Vendor will provide emergency hosting support twenty four (24) hours a day, seven days a week. Vendor will provide access to a technical representative, who can be reached twenty four (24) hours a day / seven days a week to resolve Critical and Major hosting issues as identified in table below. All other issues will be resolved during normal business hours. The following table identifies the Severity definitions of support requests and associated response/resolution times.

| Severity | Definitions or Examples |
|---|---|
| Critical | System down and not accessible, causing severe business impact to the customer. |
| Major | Major functions of the product are not working causing business impact to the customer. |
| Normal | Moderate problem or general question, such as how to read reports, how to access specific information. |
| Minor | There is a consistent and reproducible non-conformity that results in no loss of functionality and no legal or regulatory non-compliance. |
| Enhancement | Modifications that are made to application do not fall in above categories. |

Target Resolution Time – the time the problem is reported to time the problem is resolved. The resolution includes returning the system to normal operations either by the implementation of a permanent fix or a workaround.

| Severity | Target Initial Response | Target Resolution Time | Update Frequency |
|---|---|---|---|
| P1/Critical | Action on ticket within 1 business hour | Deescalate to P2 within a maximum of 12 hours | One business hour |
| P2/Major | Action on ticket within 4 business hours | 1 business day | Every 4 business hours |
| P3/Normal | Action on ticket within 1 business day | 4 business days | 2 business days |
| P4/Minor | Action on ticket within 2 business days | No target time | Weekly |
| Enhancement | Action on ticket within 2 days | Enhancement request for existing product, candidate for future core team | Weekly |

### 4.4. Deliverables

| DELIVERABLE TITLE AND REFERENCE # | DELIVERABLE DESCRIPTION |
|---|---|
| **D1.** Detailed Project Plan | An initial **draft Detailed Project Plan** must be delivered with this RFP response. The draft Detailed Project Plan provides a preliminary schedule for the project.<br>When the detailed project plan is formally accepted, the Vendor shall reestablish the scheduling baseline in the final Detailed Project Plan, and project progress shall be monitored against it. Once the Detailed Project Plan is finalized and accepted by KDHE, any updates that impact the planned end date of **ANY** phase for any specific KDHE KS-HAN activity will require an approved change request.<br>The draft and final Detailed Project Plans must include: task name, duration, work, start date, finish date, dependencies, associated Vendor and KDHE resources, and milestones. Each task shall not exceed 80 hours of work effort. Tasks that require KDHE or local agency personnel participation shall be scheduled based on normal business hours and shall be based upon a 40-hour week with the recognition that only one KDHE resource will be full time on this project. Once the project schedule is baselined, the Detailed Project Plan shall always display planned vs. actual dates and percent completion for each task. The Detailed Project Plan shall be delivered in modifiable softcopy (MS Project 2010® or later) format or similar format. |
| **D2.** Project Status Briefings | Project Status Briefings shall clearly indicate the status of each deliverable including, but not limited to, any changes to the time, quantity, or quality of each deliverable. The Project Status Briefing shall include accomplishments from the prior weeks and work to be accomplished for the next two weeks. Briefings must include attachments with an updated issues log, action items log, and risk management matrix. |
| **D3.** Service Level Agreement(s) | Proposed Service Level Agreements SLA(s) must be delivered as part of the RFP response. Review and updates to the SLA(s) are expected each time they are impacted by a change. The Vendor shall work with KDHE staff as necessary on performance level activities. The SLA(s) shall clearly delineate differences in responsibility between the Vendor's staff and KDHE staff. The SLA(s) shall minimally include:<br>• Vendor's commitment and plan with respect to ensuring that all environments are setup and maintained. Adherence to required availability and response times defined in this RFP must be stated. Vendor shall include a description of the procedures, monitoring tools, and reports used to ensure compliance with these commitments.<br>• Turnaround times for maintenance, modifications, and help desk calls are stated as Vendor commitments and monitored by the Vendor and adhered to during the pilot and the full-KDHE rollout, during maintenance and support, and during and after the introduction of any modifications, enhancements, and new releases. Vendor shall include a description of the procedures, monitoring tools, and reports used to ensure compliance with these commitments. |

| DELIVERABLE TITLE AND REFERENCE # | DELIVERABLE DESCRIPTION |
|---|---|
| | • Vendor's plan for ensuring that all other SLA(s) implied throughout this RFP, including, but not limited to, Scheduled Maintenance, Security, and Disaster Recovery, are stated as Vendor commitments and monitored by the Vendor and adhered to throughout a proposed contract and during any renewals. |
| **D4.** System Documentation | **General System Documentation** must be delivered with this RFP response on CD or softcopy (Microsoft Word and Adobe pdf, indexed format). The following categories should be included, however, additional documentation may be submitted:<br>o System Documentation including specifications and technical literature sufficient to allow a third party to maintain and operate the system, continue to develop additional functionality and upgrades to the system and provide new and ongoing user training. This technical literature must include a programmer reference to allow a third party to utilize available application programming interfaces (APIs) and web services. It must make good use of graphics and screen shots to clearly communicate functions and the user environment.<br>o Physical and logical network design documents for the proposed system environments.<br>o Description of the type of documentation support provided for each release upgrade.<br>o End-user training documentation, e.g., training materials, scripts, training evaluation forms, reports, etc.<br>Final System Documentation must be made available in editable softcopy.<br>**Final Technical Documentation** must include:<br>• System administration.<br>• Security administration.<br>• System setup and configuration.<br>**Final End-User Documentation** must include:<br>• User Reference Guide<br>• Training Materials (Training Guide, Training scripts, Training Evaluation Forms and Training Report) |
| **D5.** Solution Deployment to Test Environment | The Vendor shall implement a fully functioning version of their proposed solution (less KDHE customizations). This system will be used for demonstration and requirements gathering purposes. To be functioning, all elements documented in the contract as included in the base solution for KDHE KS-HAN shall be installed to allow data entry, viewing, and printing functions to occur. Historical data is required to be loaded. Step-by-step process of how the system shall allow data to be added via online screens or electronic batch upload. |
| **D6.** Customized Message Templates | Vendor will provide sample templates for customized messages. |
| **D7.** Data Migration | The Data Migration Plan must include high-level strategy for conducting data migration. |

| DELIVERABLE TITLE AND REFERENCE # | DELIVERABLE DESCRIPTION |
|---|---|
| Plan | |
| **D8.** Test Plan | The Vendor shall deliver Test Plan draft and final documents which clearly describe the Vendor's strategy for performing User Acceptance Testing. The Vendor shall also identify in the Test Plan all automation testing tools the Vendor plans to employ, including the specific release/version number of the product. If the Vendor plans to employ the use of automated test tools, then all test data files shall be in electronic format suitable for input to other testing tools. |
| **D9.** Automated Defect Reporting/ Tracking Process | The Vendor shall provide an automated process for reporting defects and for tracking the resolution of such defects, to include documentation and software programming defects. This process shall allow a user to report defects either by telephone or by using the Vendor's Automated Defect Reporting/Tracking online tool. |
| **D10.** Solution Deployment to Production Environment | Vendor shall deliver the current version of a fully tested and accepted production-ready system. |
| **D11.** Training Plan | An **initial Training Plan** with both program user and end-user components must be delivered with this RFP response. The Plan should include fixed price costing to cover all training broken down into daily rates. Rates will include cost breakdown for travel and lodging and cover training in two categories; technical training and user training. User training includes program-user training (KDHE staff) and end-user (public volunteer) training. In this Training Plan, Vendor will also identify the training support provided for each release upgrade. Components of the Plan should address the following training needs:<br>• Program user training – Vendor will supply training to KDHE technical staff that covers at a minimum:<br>  • System administration.<br>  • Security administration.<br>  • System setup and configuration.<br>• User training – Vendor will supply training to public volunteers.<br>  • Training recommendations based on phased rollout.<br>  • Training schedule.<br>  • Maximum number to attend each training session. |
| **D12.** Disaster Recovery Plan and participation in Disaster Recovery | A proposed Backup and Disaster Recovery Plan must be delivered with this RFP response. The Vendor, working with KDHE staff will be required to perform a Disaster Recovery Test before moving the proposed solution in the production environment. This test will demonstrate a complete systems recovery simulating a catastrophic event where all the components of the system are lost. KDHE will be the sole judge as to the success of recovery operations. Vendor will make changes as required to meet KDHE's acceptance of the recovery plan, at no cost to KDHE. The Vendor shall include in its plan strategies to work through KDHE on additional disaster recovery tests |

| DELIVERABLE TITLE AND REFERENCE # | DELIVERABLE DESCRIPTION |
|---|---|
| Testing | that include recovery of hardware, software, and the environment during this contract and any subsequent contract periods. The Vendor shall perform annual Disaster Recovery Testing to test backup and recovery as defined in the final Disaster Recovery Plan. The Vendor must submit a report of DR test results to KDHE IT. |
| **D13.** User Help Desk Services | The Vendor is required to perform system maintenance and operations, modifications, and any Help Desk functions for Vendor application support, upgrades, and release support for the proposed solution. |

### 4.5. Timeline

Vendor should make recommendations regarding a specific schedule for optimally conducting the project and delivering work products. An initial draft Detailed Project Plan must be delivered with this RFP response. The draft Detailed Project Plan provides a preliminary schedule for the project.

When the detailed project plan is formally accepted, the Vendor shall reestablish the scheduling baseline in the final Plan, and project progress shall be monitored against it. Once the detailed Project Plan is finalized and accepted by KDHE, any updates that impact the planned end date of ANY phase for any specific KDHE KS-HAN activity will require an approved change request. The final Project Plan becomes *D1. Detailed project plan* deliverable and must include: task name, duration, work, start date, finish date, dependencies, associated Vendor and KDHE resources, and milestones. Each task shall not exceed 80 hours of work effort. Tasks that require KDHE or local agency personnel participation shall be scheduled based on normal business hours and shall be based upon a 40-hour week with the recognition that only one KDHE resource will be full time on this project. Once the project schedule is baselined, Project Work Plans shall always display planned vs. actual dates and percent completion for each task. The detailed project plan shall be delivered in modifiable softcopy (MS Project 2010® or later) format.

### 4.6. State Resources

Roster of KDHE representatives working on the KS-HAN and K-Serv project.

| Name | Position |
|---|---|
| **Kim Kennedy** | IT Project Analyst |
| **Martin Miksch** | Application Developer II |
| **Samantha Ramskill** | Program Manager |
| | |

### 4.7. Payment Terms

The Vendor shall use an accounting system that meets the requirements of generally accepted accounting principles of recording and reporting receipts, obligations and disbursements.

1. Payment Terms are Net 30 days. Payments shall not be made for costs or items not listed in the vendor's response.
2. The Vendor will include a detailed invoice that includes:
2.1. Purchase order number
2.2. Description of services provided and dates of service

**5. COST SHEET**

Contractor Name:_____

Hosted solution/software package: $_____

Subsequent years maintenance and support $_____per year

## 6. Contractual Provisions Attachment

DA-146a Rev. 06/12

### 6.1. Terms Herein Controlling Provisions

It is expressly agreed that the terms of each and every provision in this attachment shall prevail and control over the terms of any other conflicting provision in any other document relating to and a part of the contract in which this attachment is incorporated. Any terms that conflict or could be interpreted to conflict with this attachment are nullified.

### 6.2. Kansas Law and Venue

This contract shall be subject to, governed by, and construed according to the laws of the State of Kansas, and jurisdiction and venue of any suit in connection with this contract shall reside only in courts located in the State of Kansas.

### 6.3. Termination Due To Lack Of Funding Appropriation

If, in the judgment of the Director of Accounts and Reports, Department of Administration, sufficient funds are not appropriated to continue the function performed in this agreement and for the payment of the charges hereunder, State may terminate this agreement at the end of its current fiscal year. State agrees to give written notice of termination to contractor at least 30 days prior to the end of its current fiscal year, and shall give such notice for a greater period prior to the end of such fiscal year as may be provided in this contract, except that such notice shall not be required prior to 90 days before the end of such fiscal year. Contractor shall have the right, at the end of such fiscal year, to take possession of any equipment provided State under the contract. State will pay to the contractor all regular contractual payments incurred through the end of such fiscal year, plus contractual charges incidental to the return of any such equipment. Upon termination of the agreement by State, title to any such equipment shall revert to contractor at the end of the State's current fiscal year. The termination of the contract pursuant to this paragraph shall not cause any penalty to be charged to the agency or the contractor.

### 6.4. Disclaimer Of Liability

No provision of this contract will be given effect that attempts to require the State of Kansas or its agencies to defend, hold harmless, or indemnify any contractor or third party for any acts or omissions. The liability of the State of Kansas is defined under the Kansas Tort Claims Act (K.S.A. 75-6101 et seq.).

### 6.5. Anti-Discrimination Clause

The contractor agrees: (a) to comply with the Kansas Act Against Discrimination (K.S.A. 44-1001 et seq.) and the Kansas Age Discrimination in Employment Act (K.S.A. 44-1111 et seq.) and the applicable provisions of the Americans With Disabilities Act (42 U.S.C. 12101 et seq.) (ADA) and to not discriminate against any person because of race, religion, color, sex, disability, national origin or ancestry, or age in the admission or access to, or treatment or employment in, its programs or activities; (b) to include in all solicitations or advertisements for employees, the phrase ""equal opportunity employer""; (c) to comply with the reporting requirements set out at K.S.A. 44-1031 and K.S.A. 44-1116; (d) to include those provisions in every subcontract or purchase order so that they are binding upon such subcontractor or vendor; (e) that a failure to comply with the reporting requirements of (c) above or if the contractor is found guilty of any violation of such acts by the Kansas Human Rights Commission, such violation shall constitute a breach of contract and the contract may be cancelled, terminated or suspended, in whole or in part, by the contracting state agency or the Kansas Department of Administration; (f) if it is determined that the contractor has violated applicable provisions of ADA, such violation shall constitute a breach of contract and the contract may be cancelled, terminated or suspended, in whole or in part, by the contracting state agency or the Kansas Department of Administration.

Contractor agrees to comply with all applicable state and federal anti-discrimination laws.

The provisions of this paragraph number 5 (with the exception of those provisions relating to the ADA) are not applicable to a contractor who employs fewer than four employees during the term of such contract or whose contracts with the contracting State agency cumulatively total $5,000 or less during the fiscal year of such agency.

### 6.6. Acceptance Of Contract

This contract shall not be considered accepted, approved or otherwise effective until the statutorily required approvals and certifications have been given.

### 6.7. Arbitration, Damages, Warranties

Notwithstanding any language to the contrary, no interpretation of this contract shall find that the State or its agencies have agreed to binding arbitration, or the payment of damages or penalties. Further, the State of Kansas and its agencies do not agree to pay attorney fees, costs, or late payment charges beyond those available under the Kansas Prompt Payment Act (K.S.A. 75-6403), and no provision will be given effect that attempts to exclude, modify, disclaim or

otherwise attempt to limit any damages available to the State of Kansas or its agencies at law, including but not limited to the implied warranties of merchantability and fitness for a particular purpose.

### 6.8. Representative's Authority To Contract

By signing this contract, the representative of the contractor thereby represents that such person is duly authorized by the contractor to execute this contract on behalf of the contractor and that the contractor agrees to be bound by the provisions thereof.

### 6.9. Responsibility For Taxes

The State of Kansas and its agencies shall not be responsible for, nor indemnify a contractor for, any federal, state or local taxes which may be imposed or levied upon the subject matter of this contract.

### 6.10. Insurance

The State of Kansas and its agencies shall not be required to purchase any insurance against loss or damage to property or any other subject matter relating to this contract, nor shall this contract require them to establish a "self-insurance" fund to protect against any such loss or damage. Subject to the provisions of the Kansas Tort Claims Act (K.S.A. 75-6101 et seq.), the contractor shall bear the risk of any loss or damage to any property in which the contractor holds title.

### 6.11. Information

No provision of this contract shall be construed as limiting the Legislative Division of Post Audit from having access to information pursuant to K.S.A. 46-1101 et seq.

### 6.12. The Eleventh Amendment

"The Eleventh Amendment is an inherent and incumbent protection with the State of Kansas and need not be reserved, but prudence requires the State to reiterate that nothing related to this contract shall be deemed a waiver of the Eleventh Amendment."

### 6.13. Campaign Contributions / Lobbying

Funds provided through a grant award or contract shall not be given or received in exchange for the making of a campaign contribution. No part of the funds provided through this contract shall be used to influence or attempt to influence an officer or employee of any State of Kansas agency or a member of the Legislature regarding any pending legislation or the awarding, extension, continuation, renewal, amendment or modification of any government contract, grant, loan, or cooperative agreement.

APPENDIX A: State and Federal Debarment Suspension Certification

Instructions for Certification:

1. By signing and submitting this proposal, the prospective primary participant is providing the certification set out below.
2. The inability of a person to provide the certification required below will not necessarily result in denial of participation in this covered transaction. The prospective participant shall submit an explanation of why it cannot provide the certification set out below. The certification or explanation will be considered in connection with the department or agency's determination whether to enter into this transaction. However, failure of the prospective primary participant to furnish a certification or an explanation shall disqualify such person from participation in this transaction.
3. The certification in this clause is a material representation of fact upon which reliance was placed when the department or agency determined to enter into this transaction. If it is later determined that the prospective primary participant knowingly rendered an erroneous certification, in addition to other remedies available to the Federal Government, the department or agency may terminate this transaction for cause of default.
4. The prospective primary participant shall provide immediate written notice to the department or agency to whom this proposal is submitted if at any time the prospective primary participant learns that its certification was erroneous when submitted or has become erroneous by reason of changed circumstances.
5. The terms "covered transaction," "debarred," "suspended," "ineligible," "lower tier covered transaction," "participant," "person," "primary covered transaction," "principal," "proposal," and "voluntarily excluded," as used in this clause, have the meanings set out in the Definitions and Coverage sections of the rules implementing Executive Order 12549. You may contact the department or agency to which this proposal is being submitted for assistance in obtaining a copy of these regulations.
6. The prospective primary participant agrees by submitting this proposal that, should the proposed covered transaction be entered into, it shall not knowingly enter into any lower tier covered transaction with a person who is debarred, suspended, declared ineligible, or voluntarily excluded from participation in this covered transaction, unless authorized by the department or agency entering into this transaction.
7. The prospective primary participant further agrees by submitting this proposal that it will include the clause titled "Certification" Regarding Debarment, Suspension, Ineligibility and Voluntary Exclusion-Lower Tier Covered Transaction," provided by the department or agency entering into this covered transaction, without modification, in all lower tier covered transactions and in all solicitations for lower tier covered transactions.
8. A participant in a covered transaction may rely upon a certification of a prospective participant in a lower tier covered transaction that is not debarred, suspended, ineligible, or voluntarily excluded from the covered transaction, unless it knows that the certification is erroneous. A participant may decide the method and frequency by which it determines the eligibility of its principals. Each participant may, but is not required to, check the Non-procurement List.
9. Nothing contained in the foregoing shall be construed to require establishment of a system of records in order to render in good faith the certification required by this clause. The knowledge and information of a participant is not required to exceed that which is normally possessed by a prudent person in the ordinary course of business dealings.
10. Except for transactions authorized under paragraph 6 of these instructions, if a participant in a covered transaction knowingly enters into a lower tier covered transaction with a person who is suspended, debarred, ineligible, or voluntarily excluded from participation in this transaction, in addition to other remedies available to the Federal Government, the department or agency may terminate this transaction for cause or default.

APPENDIX A: State and Federal Debarment Suspension Certification

Certification Regarding Debarment, Suspension, and Other Responsibility Matters - Primary Covered Transactions

1. The prospective primary participant certifies to the best of its knowledge and belief, that it and all its principals:

(a) Are not presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from covered transactions by any Federal or State department or agency;
(b) Have not within a three-year period preceding this proposal been convicted of or had a civil judgment rendered against them for commission of fraud or a criminal offense in connection with obtaining, attempting to obtain, or performing a public (Federal, State or local) transaction or contract under a public transaction; violation of Federal or State antitrust statues or commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, or receiving stolen property;
(c) Are not presently indicted for or otherwise criminally or civilly charged by a governmental entity (Federal, State or local) with commission of any of the offenses enumerated in paragraph (1) (b) of this certification; and
(d) Have not within a three-year period preceding this application/proposal had one or more public transactions (Federal, State or local) terminated for cause or default.

2. Where the prospective primary participant is unable to certify to any of the statements in this certification, such prospective participant shall attach an explanation to this proposal.

APPENDIX B: Requirements Table

Fit Rating Response Codes:
5 = Requirement Fully Met (No System Customization Needed) 2 = Alternative Approach to Requirement (describe Approach in Response)
4 = Requirement Partially Met (Describe System Customization Needed) 1 = No Solution Proposed (Describe Why in Response)
3 = Requirement Not Met (Describe Capability to Develop)

| **Reference #** | **Requirement Description**<br>Requirements listed in this Table are intended for Vendor consideration in their SOW Response. Vendors should use this Table to score the degree to which the Proposed System functionality and supporting Vendor capabilities meet each requirement. Any narrative descriptions should be compiled in an attachment and cross-referenced to this Table. | Fit Rating Response (must provide comment to support response) | Comments Supporting Response | **Vendor Document Reference** |
|---|---|---|---|---|
| B Basic Requirements | | | | |
| B1 | Broadcasts messages to any communications device including mobile devices, desktops and websites. Support for multi-platform smart phones and tablets including Apple® iOS and Android™ devices. | | | |
| B2 | Ability to create notification templates with pre-determined contact lists and pre-defined messages. | | | |
| B3 | Automated bulk, partial and full updates of contacts utilizing a secure, industry-standard method for data transfer. | | | |
| B4 | Search or filter contacts on any attribute or combination of attributes within a contact's profile. | | | |
| B5 | Notify contacts and/or manage contact data across multiple distributed data stores from a single access point. | | | |
| B6 | Ability to upload existing customer profile data into system. | | | |
| B7 | Ability to customize what data is collected for customer profiles. | | | |
| B8 | Ability to conduct surveys via notification system. | | | |

Fit Rating Response Codes:
5 = Requirement Fully Met (No System Customization Needed) 2 = Alternative Approach to Requirement (describe Approach in Response)
4 = Requirement Partially Met (Describe System Customization Needed) 1 = No Solution Proposed (Describe Why in Response)
3 = Requirement Not Met (Describe Capability to Develop)

| **Reference #** | **Requirement Description**<br>Requirements listed in this Table are intended for Vendor consideration in their SOW Response. Vendors should use this Table to score the degree to which the Proposed System functionality and supporting Vendor capabilities meet each requirement. Any narrative descriptions should be compiled in an attachment and cross-referenced to this Table. | Fit Rating Response (must provide comment to support response) | Comments Supporting Response | **Vendor Document Reference** |
|---|---|---|---|---|
| B9 | Ability to receive acknowledgement of notifications. | | | |
| B10 | Persistent notifications when alerts go unanswered. | | | |
| B11 | Ability to create and join call bridge from notifications. | | | |
| G Geospatial Requirements | | | | |
| G1 | Provide GIS-based message targeting defined by zip code, street address, radius from a specific point, or other attribute. | | | |
| G2 | Save and organize critical and often-used geo-shapes and boundaries. | | | |
| G3 | Create or import geo-regions for one-time use or categorize and store in region library for reuse later. | | | |
| G4 | Dynamic search, filtering and targeted alerts to view the locations of special needs populations, subscribers to specific alert types, fire districts, police stations, and more. | | | |
| G5 | Load, geo-code and manage contact data within a single interface in real-time. | | | |
| G6 | Search address, location or point-of-interest and exclude contacts based on location or other attributes. | | | |

Fit Rating Response Codes:
5 = Requirement Fully Met (No System Customization Needed) 2 = Alternative Approach to Requirement (describe Approach in Response)
4 = Requirement Partially Met (Describe System Customization Needed) 1 = No Solution Proposed (Describe Why in Response)
3 = Requirement Not Met (Describe Capability to Develop)

| **Reference #** | **Requirement Description**<br>Requirements listed in this Table are intended for Vendor consideration in their SOW Response. Vendors should use this Table to score the degree to which the Proposed System functionality and supporting Vendor capabilities meet each requirement. Any narrative descriptions should be compiled in an attachment and cross-referenced to this Table. | Fit Rating Response (must provide comment to support response) | Comments Supporting Response | **Vendor Document Reference** |
|---|---|---|---|---|
| G7 | Upload display-only shapefiles identifying critical resources such as facility locations, oil pipelines, transmission lines, critical resource depots, etc. for reference on the map. | | | |
| R Reporting Requirements | | | | |
| R1 | Customizable reporting and analytics | | | |
| R2 | Ability to create and launch frequently requested reports | | | |
| R3 | Ability to export reports with off-line creation of pivot tables and cross-referencing. | | | |
| R4 | Detailed notification analysis report for quick and easy broadcast review. | | | |
| S Security Requirements | | | | |
| S1 | Provide Audit logs of changes made within the system. | | | |
| S2 | Ability to store and send Personally Identifiable Information (PII) data locally and securely to comply with Kansas regulatory requirements | | | |
| S3 | Provide Encryption of data at rest. | | | |

Fit Rating Response Codes:
5 = Requirement Fully Met (No System Customization Needed) 2 = Alternative Approach to Requirement (describe Approach in Response)
4 = Requirement Partially Met (Describe System Customization Needed) 1 = No Solution Proposed (Describe Why in Response)
3 = Requirement Not Met (Describe Capability to Develop)

| **Reference #** | **Requirement Description**<br>Requirements listed in this Table are intended for Vendor consideration in their SOW Response. Vendors should use this Table to score the degree to which the Proposed System functionality and supporting Vendor capabilities meet each requirement. Any narrative descriptions should be compiled in an attachment and cross-referenced to this Table. | Fit Rating Response (must provide comment to support response) | Comments Supporting Response | **Vendor Document Reference** |
|---|---|---|---|---|
| S4 | Role-based access controls for organization administrators, group managers, data managers, dispatchers and notification operators. | | | |
| S5 | Secure user authentication | | | |
| S6 | Provide ability for administrator to reset user password, reinstate a user, and disconnect or logout a user. | | | |
| H Hosting Functions | | | | |
| H1 | Provide 24 hours per day and 7 days per week live support. | | | |
| H2 | Provide 98.9% uptime availability of notification system. | | | |
| H3 | Vendor shall establish and maintain up to three (3) processing environments. These processing environments are:<br>1) Production – Versions of released, fully tested and user accepted code. Requires stringent change management and monitoring controls and processes.<br>2) Testing/QA – This environment will be the initial staging area for testing upgrade/update components (scripts, data conversions, etc). Activities in this environment may contain an accumulation of incremental updates as a rollup package accepted in the Development environment. After final | | | |

Fit Rating Response Codes:
5 = Requirement Fully Met (No System Customization Needed) 2 = Alternative Approach to Requirement (describe Approach in Response)
4 = Requirement Partially Met (Describe System Customization Needed) 1 = No Solution Proposed (Describe Why in Response)
3 = Requirement Not Met (Describe Capability to Develop)

| **Reference #** | **Requirement Description**<br>Requirements listed in this Table are intended for Vendor consideration in their SOW Response. Vendors should use this Table to score the degree to which the Proposed System functionality and supporting Vendor capabilities meet each requirement. Any narrative descriptions should be compiled in an attachment and cross-referenced to this Table. | Fit Rating Response (must provide comment to support response) | Comments Supporting Response | **Vendor Document Reference** |
|---|---|---|---|---|
| | acceptance, this environment will serve as the on-going Development Testing/QA environment. Testing should mirror the Development environment plus include the same security infrastructure components as Production to allow technical staff to fully ensure secure application and data access requirements are met.<br>3) Disaster Recovery - Mirrors the production environment with hardware and software requirements. Will serve as a backup to the production environment if production environment is deemed unusable. This environment must be located in different city than production system. | | | |
| H4 | Provide Regular Backup and Recovery Services. | | | |
| H5 | Provide administration of all security devices, i.e., firewalls and, secure authentication server. | | | |
| H6 | Availability to 105 local health departments and up to 171 hospitals in Kansas. | | | |
| H7 | All hosting vendors for KDHE must complete three (3) “Cloud Service Provider” documents to meet KDHE hosting requirements. These documents are located in **APPENDIX C**. | | | |

| T Technical Requirements | | | | |
|---|---|---|---|---|
| T1 | Browser-based access using Internet Explorer version 9.0 or greater. | | | |
| T2 | Ability to conform to KDHE server operating system standard (MS/Windows Server 2008 or greater) or propose an alternative solution and the rational for using a different server operating system. | | | |
| T3 | Ability to conform to KDHE database engine standard (MS/SQL Server 2012) or propose an alternative solution and the rational for using a different database engine. | | | |
| T4 | Easy refreshing of test and training data, on demand, by system administrator or qualified database administrator. | | | |
| T5 | Accurate/current data and meta-data dictionary available. | | | |
| T6 | Database support data replication and synchronization across multiple physical servers. | | | |
| T7 | Provide recommended hardware configurations based on contact population. | | | |
| T8 | Provide Application Programming Interfaces (API) | | | |
| T9 | Ability to interface with Kansas online training system called KS-Train at https://ks.train.org/ | | | |
| T10 | Web-based applications shall NOT:<br>• User shared folders or network drives<br>• User parental paths<br>• Query information or hierarchy paths via the query string. | | | |
| T11 | Web Accessibility shall:<br>• Conform to Information Technology Policy 1210 Revision 2, State of Kansas Web Accessibility Requirements and Section 508 of the Rehabilitation Act (29 U.S.C. 794d) regarding American Disabilities Act compliance guidelines. Developers may research this information at http://www.da.ks.gov/kpat/policy/.<br>Vendor response will indicate their ability to conform to this requirement or propose an alternate solution and the rationale. | | | |

| | | | | |
|---|---|---|---|---|
| T12 | Ability to operate across State's 100 MB WAN and 10/100/1000 LAN or propose an alternative solution and the rationale for using a different configuration. | | | |
| T13 | Ability to support up to 5000 concurrent users. | | | |

**APPENDIX C: Cloud Service Provider Documents**

**Name of Vendor** _____

## Cloud Service Provider Questionnaire

1. Does the Cloud Service Provider (CSP) have a secure environment, federally authorized to at least the standards of confidentiality and integrity from the Moderate FIPS-199 level to store records containing Personal Identifiable Information (PII)?

2. Does the Cloud provider have the ability to alter Terms of Service or contracts without the express written consent of the customer agency?

3. Will the ownership of data remain under the sole ownership of the State of Kansas at all times?

4. Will backup information be returned to the State of Kansas in the event the contract is ended or the Cloud provider files for bankruptcy?

5. Is there a documented process to address the removal and control of agency information upon the termination of the contract between the agency and the cloud provider?

6. Can the cloud provider utilize any data stored on their systems for any purpose outside agency use?

7. Does the contract contain language to restrict the sharing of privacy data with any entity not explicitly authorized in the contract?

8. Does the contract contain language to restrict the storage, transfer, or processing of privacy data to only facilities that fall under the legal jurisdiction of the United States?

9. What controls are in place to prevent the misuse of data by those having access?

10. Does the cloud provider allow for access to data as permitted under current federal and Kansas law to both authorized federal agencies and individuals wishing to verify their own PII?

11. While the data is with the cloud provider, what are the requirements for determining if the data is sufficiently accurate, relevant, timely, and complete to ensure fairness in making determinations?

12. Describe what privacy training is provided and who is responsible for protecting the privacy rights of the users of the cloud?

13. How does the cloud provider facilitate response to Kansas Open Records Act (KORA) / Federal Open Information Act (FOIA) / subpoena requests?

14. Is there a complete and documented process to report and handle breaches?

15. Describe the process that the CSP will use to report, within 1-hour, any potential privacy or security breaches to the agency regardless of whether the breach was intentional or inadvertent.

16. Describe the specific redress actions that the agency can take against the cloud provider in the event of a breach

**APPENDIX C: Cloud Service Provider Documents**

**Instructions for Completing the Web-Enabled Application Security Questionnaire**
Vendor will complete this questionnaire by responding to all questions to the best of their ability.

| **Web-Enabled Application Security Questionnaire for:** *Vendor Name* **Date:** / / | | |
|---|---|---|
| **Physical Security**- involves the security of the physical devices, which includes the ability to control access to such hardware. | | |
| # | **Question** | **Response** |
| 1 | What are the hardware components and where are they physically located? | |
| 2 | Who has access to the physical components? | |
| 3 | Are the environmental controls adequate (i.e., smoke and water detection, fire prevention)? | |
| 4 | What UPS is being used and what characteristics does it have? | |
| **User Security**- addresses the ability to ensure that the user accessing data and systems is in fact who they say they are and that they have access only to those resources to which they are authorized. Functions that are involved in this issue include identification, authentication, and authorization of the individual, as well as non-repudiation and audit. | | |
| # | **Question** | **Response** |
| 5 | How are users identified to the systems? | |
| 6 | What unique form of identification do they have (UserID) ? | |
| 7 | Who administers the UserIDs? | |
| 8 | How are inactive users removed, by whom, and how timely? | |
| 9 | How are users authenticated to the system (passwords, smart cards, biometrics)? | |
| 10 | If passwords are used, what are the specific password rules (minimum length, character makeup, aging, etc)? | |
| 11 | How is assurance provided that the information received has not been altered? | |
| 12 | How is assurance provided that the reputed sender is indeed the one who sent it? | |
| 13 | What levels of system access are there? | |
| 14 | Who determines and maintains? | |
| 15 | What audit trails are maintained to enable reconstruction and/or review of operations performed on systems? | |
| 16 | How are they protected so users can not change them? | |
| 17 | How often are they reviewed and by whom? | |
| **Application Security**- concerns the built-in security features of the application itself. | | |
| # | **Question** | **Response** |
| 18 | What security features are built into the application? | |
| 19 | How specifically do the security features work? | |
| 20 | If the application communicates to other systems, how does that happen? (i.e.. web server to database server). | |

| **Web-Enabled Application Security Questionnaire for:** *Vendor Name* **Date:** / / | | |
|---|---|---|
| 21 | Has **auto complete = off** been set for all input fields on applications using IE 5.0 or above.? | |
| 22 | What information is logged for each transaction? (The minimum is userID, IP Address, and time and date stamp) | |
| 23 | Where is the logging information stored? | |
| 24 | Does the application use session tokens that are custom created or default from a Vendor, i.e.. Microsoft? (All session tokens shall be user unique, non-predictable, and resistant to reverse engineering.) | |
| 25 | Does the application store any cookies on client machines? If so, what are they? | |
| 26 | Are cookies checked for validity when returned back to the server? | |
| 27 | Are sessions and/or cookies destroyed when the user logs out of the application? | |
| 28 | Does the application require re-authentication for critical user actions such as money transfer? | |
| 29 | What security controls are built around files where userIDs, passwords, Pins, etc are stored? | |
| 30 | Are all authentication events (logging in, logging –out, failed logins, etc.) logged? | |
| 31 | Are all administrative events (account management actions, enabling or disabling logging, etc.) logged? | |
| 32 | Are logs written so only new records can be added, and existing records not overwritten or deleted? | |
| 33 | What client-side data validation is done? | |
| 34 | What data validation is done on the server side? (this shall be done even if it is redundant to cursory validation performed on the client side). | |
| 35 | How is editing done to prohibit generic meta-characters from being present in input data? | |
| 36 | Are all database queries constructed with parameterized stored procedures to prevent SQL injection? | |
| 37 | Can any variables be used in script? If yes, how are they protected to prevent direct OS Commands attacks? | |
| 38 | What scripting language is being used? Has it been checked for vulnerabilities and have they been addressed? | |
| 39 | Does the application do security checking after UTF-8 decoding is completed? | |

| **Web-Enabled Application Security Questionnaire for:** *Vendor Name* **Date:** / / | | |
|---|---|---|
| 40 | Have all comments been removed for any code passed to the browser? | |
| 41 | Can users see any debugging information on the client? | |
| 42 | Have all sample, test and unused files been removed from the production system? | |
| 43 | Are pages with personal data cached? | |
| 44 | Are forms submissions done using a POST request rather than a GET? | |
| 45 | Does IUSR and/or network services need write permissions to any folders? If so, which ones and why? | |
| 46 | Does IUSR and/or Network Service need read and/or write access to the registry beyond the defaults? | |
| 47 | Does your application require any shared folders? | |
| 48 | Are all your connection string information(passwords & user names) stored in the registry and not in the application? | |
| 49 | Does your application need parental paths on in the IIS server? | |
| 50 | Does your application use stored procedures for database interaction? | |
| 51 | Do you follow ADA guidelines in your presentation layers of your application? | |
| 52 | Does your application require any 3rd party software that is not a standard part of our Microsoft operating system? | |
| 53 | Does your web application adhere to a three layer architecture (Presentation, Business and Data)? | |
| **System Security**-involves the analysis of the overall operating systems and software used to support the applications software. | | |
| **#** | **Question** | **Response** |
| 54 | What research has been done for known security vulnerabilities? | |
| 55 | Who installs Vendor-supplied security upgrades and patches? Are we up-to-date? | |
| 56 | Have unnecessary services been removed or disabled? | |
| 57 | Has debugging mode on any web server been turned off for production? | |
| 58 | Are default accounts disabled and passwords changed from defaults? | |
| 59 | Does the data base user have limited abilities in being only able to run stored procedures or select? | |
| **Data Security**-encompasses both physically protecting the application data from unauthorized access as well as loss of data through mechanical/electrical failure or viruses | | |
| **#** | **Question** | **Response** |
| 60 | Is Authentication used at all times when accessing or making changes to data to ensure confidentiality? | |

| **Web-Enabled Application Security Questionnaire for:** *Vendor Name* **Date:** / / | | |
|---|---|---|
| 61 | Is at least 128-bit encryption used for any data transmitted over public networks? | |
| 62 | Are all FTP transmissions of data over insecure channels encrypted using PGP software? | |
| 63 | Is auditing activated and all access to data logged? | |
| 64 | What are the backup and archive procedures that will be used? | |
| 65 | What are the offsite storage requirements of backups and archives? | |
| 66 | Are backups encrypted if highly sensitive data is involved? | |
| 67 | What virus control software and detection procedures will be used to protect the data? | |
| 68 | How is privacy maintained to ensure that customer's personal data collected from electronic transmissions is protected from unauthorized transmissions? | |
| **Network Security**-.includes the physical/electrical links between the Desktop Client and the Host computer | | |
| # | **Question** | **Response** |
| 69 | What documents show the network environment with a diagram that shows all links and component parts? | |
| 70 | How is the LAN isolated from any network-connected device that does not have a valid business relationship with resources on the LAN? | |
| 71 | Are firewalls used between the LAN and the Internet to prevent untrusted networks from accessing the LAN? | |
| 72 | If public access to a server in the internal LAN is required, has the server been put on a separate LAN segment behind the firewall device typically referred to as the DMZ? | |
| 73 | Have intrusion detection systems been installed? | |
| 74 | How are they monitored for unauthorized access? | |
| **Security Administration**- involves the administration of the overall security plan | | |
| # | **Question** | **Response** |
| 75 | Who are the security administrators for the application? | |
| 76 | What functions do they provide? | |
| 77 | How are users provided with userIDs and passwords? | |
| 78 | Are passwords restricted from being distributed by telephone or unsecured electronic mail? | |
| 79 | How are unusual incidents handled? | |
| 80 | Have all employees or users of the application been instructed to exercise caution to prevent the release of sensitive details to unauthorized sources? | |

| **Web-Enabled Application Security Questionnaire for:** *Vendor Name* **Date:** / / | | |
|---|---|---|
| **Database Security: involves the connections to the database** | | |
| **#** | **Question** | **Response** |
| 81 | Do you pass SQL query information or hierarchy paths via the request objects? | |
| 82 | Does your application use server side validation for sensitive, financial, or authorization information input before disseminating, writing, updating or allowing access to the application or database? | |

**APPENDIX C: Cloud Service Provider Documents**

**Vendor Name** _____

**Date** _____

1. Introduction

    1.1. Add Text.

2. Architecture Overview

    2.1. Add Text.
    2.2. Add diagram.

3. Architectural Layers

    3.1. Add Text.
    3.2. Add diagram.

4. Logical Architecture

    4.1. Add text.
    4.2. Add diagram.

5. Deployment Architecture

    5.1. Add text.
    5.2. Add diagram.

6. Disconnected Operations

    6.1. Add text.
    6.2. Add diagram.

7. Security

    7.1. Add text.
    7.2. Add diagram.

8. Microsoft Enterprise Library

    8.1. Add text.

9. Operational Considerations

    9.1. Add text.

APPENDIX D: Vendor Employee Computer and Network User Agreement

All employees of vendors and Vendors who will access Kansas Department of Health and Environment (KDHE) information systems in the normal course of their work for the State of Kansas are required to sign this Vendor Employee Computer and Network User Agreement document and Confidentiality and Access Agreement before accessing any KDHE computer system.

- All vendor personnel shall use only accounts authorized by the KDHE Office of Information Services (OITS) Chief Information Office (CIO) or designee.
- Vendor personnel may access only those resources for which they are specifically authorized.
- Vendor personnel are personally responsible for safeguarding their account and log-on information. Passwords shall adhere to the password management procedure for the applicable system.
- Passwords shall never be displayed, printed, or otherwise recorded in an unsecured manner.
- Vendor personnel are not permitted to script their user IDs and passwords for log-on access.
- Vendor personnel are not permitted to allow another person to log-on to any computer utilizing their, if provided, personal account, nor are they permitted to utilize someone else's account to log-on to a computer. Authorized system or service accounts maybe used by multiple people.
- Vendor personnel may not leave their workstation logged onto the network while away from their area. Vendor personnel may elect to lock the workstation rather than logging off when leaving for very short time periods.
- Vendor personnel shall maintain a log, left with the computer and/or emailed to the KDHE OITS CIO or designee, of all software loaded onto any KDHE computer. The software must have been approved in writing by the KDHE OITS CIO or designee.
- Vendor personnel shall execute only applications that pertain to their specific contract work.
- Vendor personnel shall promptly report log-on problems or any other computer errors to the KDHE OITS CIO or designee.
- Vendor personnel shall promptly notify the KDHE OITS CIO or designee and the program project manager (data owner) if they have any reason to suspect a breach of security or potential breach of security.
- Vendor personnel shall promptly report anything that they deem to be a security loophole or weakness in the computer network to the KDHE OITS CIO or designee.
- Vendor personnel may not copy any software from any KDHE computer system for personal use.
- KDHE data shall not be removed from the premises without prior written approval from the KDHE OITS CIO or designee and the data owner.
- Vendor personnel may not remove from the KDHE premises, any computer hardware for any reason, without written permission from the KDHE OITS CIO or designee. KDHE computer systems (servers, desktop and laptop computers) may contain KDHE information or data that might be sensitive.
- Vendor personnel shall not install or use any type of encryption device or software that has not been approved in writing by the KDHE OITS CIO or designee, for use on their computer system.
- Vendor personnel shall not delete or disable any authorized encryption device or software program installed on KDHE hardware.
- Vendor personnel shall not attach any device to the KDHE network without written approval from the KDHE OITS CIO or designee.
- Vendor personnel shall not attach any network or phone cables to any device without written approval from the KDHE OITS CIO or designee.
- Vendor personnel may not disable or bypass any anti-virus program.

- Vendor personnel may not utilize KDHE computer systems for any of the following reasons:
  - Game playing;
  - Internet surfing not required for their work activity;
  - Non-related work activity; or
  - Any illegal activity.
  - Downloading of files from the Internet. If files are needed for your work, contact KDHE personnel.
- Vendor personnel are prohibited from intercepting or monitoring network traffic by any means, including the use of network sniffers, unless authorized in writing by the KDHE OITS CIO or designee.
- Vendor personnel may not give out any KDHE computer information to anyone. Exception: other vendor personnel needing the information to complete tasks and who have signed this agreement. Information includes but is not limited to: IP addresses, security configurations, etc.
- All data storage media shall be erased or destroyed prior to being placed in the trash.
- Vendor personnel are prohibited from causing the KDHE or the State of Kansas to incur any expenses unless approved in writing by the KDHE OITS CIO or designee and the program project manager (data owner
- Vendor personnel may not remove or delete any computer software without the written approval of the KDHE OITS CIO or designee.
- Vendor personnel shall not attempt to obtain or distribute KDHE system passwords.
- Vendor personnel shall not attempt to obtain or distribute door passcodes to secured rooms at the KDHE facilities.
- Vendor employees may not use the KDHE's email system to send or receive obscene, abusive, sexually explicit language or pictures, or threatening language.
- Vendor employees are prohibited from causing the KDHE, or the State of Kansas to break copyright laws.
- Vendor shall document the employee who logged on to KDHE computer systems if a shared account is used. This can be done in the vendor's help desk ticket system.
- Vendor shall not create and/or install any backdoor to any KDHE information systems to allow or gain access other than through authorized means.
- Vendor employee has read and accepts KDHE Internal Directive 7001.0 and 7002.0.
- Vendor employee has read and will comply with Information Technology Policy 7400 – Computer Security Awareness and Training.

---

Use of any part of the KDHE's computer network will acknowledge acceptance of the above policies.

Any vendor employee who violates any of the above policies shall be subject to disciplinary action, including but not limited to total removal from the KDHE project, assessed fees for damages, as well as being subject to Kansas's civil and criminal liability. Disciplinary action may include the KDHE requesting the vendor consider demotion, suspension and termination.

| _____ | _____ | _____ |
|---|---|---|
| Vendor Name - Printed | Authorizing Employee Name Printed | Date |

_____

Employee Signature

Curtis State Office Building
1000 SW Jackson St., Suite 540
Topeka, KS 66612-1367

Kansas

Phone: 785-296-0461
Fax: 785-368-6368
www.kdheks.gov

Robert Moser, MD, Secretary | Department of Health & Environment | Sam Brownback, Governor

**December 14, 2012**

**KDHE Internal Directive 7001.0**
**Subject**: Kansas Department of Health and Environment Technology Acceptable Use Policy
**Reference:** KDHE Internal Directive 7002.0 KDHE Information Technology Security Policy

1) **Purpose.** The goal of this policy is to define the appropriate use of all computers issued by KDHE to agency personnel, Vendors, and other parties.

2) **Discussion.** This directive was created to mitigate known risks associated with: a breach of confidentiality or integrity due to the access, transmission, storage, and disposal of sensitive information using a computer and/or a loss of availability to critical systems as a result of using a computer. The use of all KDHE-issued computers shall be governed by this directive. All users of KDHE-owned computers are required to follow the procedures identified in this directive.
   a) **Definitions**
      i) KDHE: Kansas Department of Health and Environment
      ii) OITS: Office of information Technology Services
      iii) Encryption: A process that encrypts the data stored on a device
      iv) WLAN: Wireless Local Area Network
      v) Restricted Data: Data is classified as Restricted when the unauthorized disclosure, alteration or destruction of that data could cause a significant level of risk to KDHE or its affiliates. Examples of Restricted data include data protected by state or federal privacy statutes and/or regulations and data protected by confidentiality agreements. The highest level of security controls should be applied to restricted data. By default, all Agency Data that is not explicitly classified as Public data should be treated as restricted data.
      vi) Public Data: Data is classified as Public when the unauthorized disclosure, alteration or destruction of that data would results in little or no risk to KDHE and its affiliates. Examples of Public data include press releases, Agency public websites and Agency publications. While little or no controls are required to protect the confidentiality of Public data, some level of control is required to prevent unauthorized modification or destruction of Public data.

**3) Procedures.**
   **a) Device Management**
      **i)** KDHE-issued computers are for the exclusive use of the agency to conduct KDHE business computer capabilities. Users are authorized to use KDHE-issued computers and computer related equipment in the manner designed by the manufacturer to conduct official business in the performance of their duties as KDHE employees and/or Vendors.
      **ii)** KDHE computers may be used to access the internet and other public information technology resources in conformance with the Access Control in this policy.
      **iii)** KDHE computers are the sole property of the agency and must be surrendered to KDHE OITS at the direction of the Agency appointing authority.

**iv)** Only approved KDHE IT personnel may administer the settings on KDHE-issued computer devices requiring local administrator authority. This includes but is not limited to:
(1) Device Operating System Installation
(2) Device System Settings
(3) Software Installation
(4) Electronic Mail Settings (Does not include user preferences)
(5) Purchased/Installed Applications
(6) Passwords that control the above settings

**b) Access Control**

i) The use of KDHE-issued computers may not be in a matter or for a purpose that would reflect unfavorably upon KDHE's reputation such as use of illegal, unethical, or sexual activities, or gambling or organized wagering.

ii) The use of KDHE-issued computers must comply with any laws, regulations, and KDHE policies, standards, and guidelines. The use of KDHE-issued equipment for violating any local, state, or federal statute is prohibited.

iii) KDHE-issued computers can be used for personal use only on a very limited basis at the discretion of the supervisor and must not interfere with work responsibilities.

iv) The use of KDHE-issued computers must not interfere with required business communications.

v) The use of KDHE-issued computers must not be used to support any business other than that of Kansas Government.

vi) The use of KDHE-issued computers must not result in monetary charges to KDHE for non-work related items. Only approved software can be installed and used on KDHE computers. Contact KDHE OITS for approval and installation of approved applications on KDHE computers.

vii) Only approved cloud services provider solutions can be installed and/or accessed using KDHE computers. Contact KDHE OITS for approval and installation/configuration of approved cloud service offerings on KDHE computers.

viii) Only KDHE OITS staff is authorized to install software on KDHE computers requiring local administrator authority.

ix) Users must lock their computer when leaving it unattended.

x) Users will not allow unattended access to KDHE-issued computers by another user except as necessary to perform upgrades and maintenance on the computer or as authorized by the KDHE OITS Security Officer. The use of KDHE-issued equipment for YouTube and Social Media sites such as Facebook and other non-work blog sites is prohibited unless specifically authorized by the KDHE Chief Information Officer and the KDHE Public Information Officer.

xi) The use of KDHE-issued equipment for writing or forwarding chain letters is prohibited.

xii) The use of KDHE-issued equipment to lobby elected officials is prohibited.

xiii) The use of KDHE-issued equipment to access personal e-mail accounts such as Hotmail, Yahoo, etc. is prohibited.

xiv) Sending e-mails to "All KDHE Staff' and "Curtis Downtown" distribution lists will NOT be permitted except by designated employees.

xv) All streaming video or audio music not required to conduct official business on a KDHE-issued computer is strictly prohibited unless authorized by the KDHE Chief Information Officer.

xvi) The KDHE OITS will respond in writing to all KDHE requests for authorization to use KDHE computers in a manner not expressly allowed by the KDHE Acceptable Use Policy and maintain a record of such authorization with the KDHE Information Security Office.

**c) Authentication**

**i)** KDHE employee's network and computer account information must not be shared and group-network and computer accounts shall not be permitted, except when required by specific applications or computer platforms, and must be pre-approved by the KDHE Information Security Officer.

**d) Encryption**

**i)** The use of encryption may be required for KDHE computers that store or access sensitive information.

**ii)** The use of encryption is required for the transmission of restricted data to/from KDHE-issued computers.

**e) Incident Detection and Response**

**i)** KDHE computer users are required to immediately report the loss of control over any computer to KDHE OITS. Reporting the loss of control of a KDHE-issued computer outside of normal working hours will be made by contacting the KDHE Chief Information Officer or his/her designee by calling the OITS Central Office Network Operations Center at 785-296-2310.

**ii)** KDHE-issued portable computers will have the capability for KDHE OITS to remotely wipe and/or track their location on demand.

**f) User Responsibilities**

**i)** Personal computers are prohibited access to KDHE business and information technology systems unless authorized by the KDHE Chief Information Officer or his/her designee. Only computers issued by KDHE are authorized to access KDHE information technology resources.

**ii)** Agency personnel issued a KDHE computer will conform to KDHE security and acceptable use policies when using the computer to access the internet and other public information technology resources.

**iii)** Users acknowledge that they have no expectation of privacy on KDHE-issued computers.

**iv)** User acknowledges KDHE retains ownership of all data stored on KDHE-issued computers.

**v)** User acknowledges that any non-agency data created and/or stored on the KDHE-issued computer becomes the property of KDHE and will be governed by the KDHE data retention and disclosure policy.

**vi)** Users will physically secure the computer when left unattended. When left in a car, a KDHE-issued portable computer will be hidden from view.

**vii)** KDHE personnel are required to return KDHE-issued computers at the end of employment.

**viii)** KDHE users are prohibited from using a KDHE-issued computer while operating a motor vehicle.

**ix)** KDHE-issued computers should not be physically or wirelessly connected to any non-KDHE devices or networks except as approved by the KDHE Office of Information Technology Services.

**x)** All KDHE-issued computers shall be protected with a firewall and anti-virus software.

**xi)** No KDHE employees shall disrupt or disable software updates from KDHE OITS.

**xii)** No "Inappropriate files" will be copied or used in any manner that involves the KDHE network. These include non-business-related MP3s, GIF files, games, executables, document files, and any other software not approved by the KDHE Chief Information Officer.

**xiii)** KDHE users shall contact the KDHE Help Desk to request approval to use KDHE issued computers for any use not specifically identified in this policy or for uses requiring KDHE Office of Information Technology Services approval.

4) **Action.**

**a)** This directive applies to all computers and all computer devices issued by KDHE.

**b)** Any exceptions to the prescribed procedures must be approved by the KDHE Chief Information Officer or their designee.

**c)** Any deviation from the prescribed procedures in the KDHE Acceptable Use Policy, the KDHE Information Technology Security Policy or other use as authorized by the KDHE OITS, subjects the user to disciplinary action under State of Kansas Personnel Policy and Procedures.

**d)** Any use not specifically identified in this policy is prohibited without prior authorization by KDHE OITS.

Robert Moser, M.D., Secretary
Department of Health and Environment

12/19/12
Date

Curtis State Office Building
1000 SW Jackson St., Suite 540
Topeka, KS 66612-1367

Kansas

Phone: 785-296-0461
Fax: 785-368-6368
www.kdheks.gov

Robert Moser, MD, Secretary

Department of Health & Environment

Sam Brownback, Governor

December 14, 2012

KDHE Internal Directive 7002.0

Subject: Kansas Department of Health and Environment Information Technology Security Policy

Reference: KDHE Internal Directive 7001.0 KDHE Information Technology Acceptable Use Policy

1) **Purpose.** The goal of this policy is to establish rules to assure the protection of confidential and/or sensitive information stored or transmitted electronically and to ensure the protection of KDHE's information technology resources.

2) **Discussion.** This directive was created to protect KDHE information assets. This is a process, which incorporates many compensating controls. Standard information security policies require that agencies identify, classify and protect the automated files, databases and applications that they own. Identifying and classifying information and the applications that function to process it is at the heart of identifying and selecting appropriate security and risk management practices. KDHE's security objective shall include maintaining information integrity and confidentiality while assuring the availability of critical information technology. Information is a critical and vital asset, and all access to, uses of and processing of KDHE information must be consistent with agency policies and standards.
   a) **Definitions**
      i) KDHE: Kansas Department of Health and Environment
      ii) OITS: Office of Information Technology Service
      iii) CIO: Chief Information Officer
      iv) IT: Information Technology
      v) Shared Drive: A KDHE network directory with access controls used as a repository for documents that only defined agency users can access.
      vi) Data Owner: The KDHE program area responsible for determining appropriate access and appropriate use of agency data stores.
      vii) Restricted Data: Data is classified as Restricted when the unauthorized disclosure, alteration or destruction of that data could cause a significant level of risk to KDHE or its affiliates. Examples of Restricted data include data protected by state or federal privacy statutes and/or regulations and data protected by confidentiality agreements. The highest level of security controls should be applied to restricted data. By default, all Agency Data that is not explicitly classified as Public data should be treated as restricted data.
      viii) Public Data: Data is classified as Public when the unauthorized disclosure, alteration or destruction of that data would results in little or no risk to KDHE and its affiliates. Examples of Public data include press releases, Agency public websites and Agency publications. While little or no controls are required to protect the confidentiality of Public data, some level of control is required to prevent unauthorized modification or destruction of Public data.

3) **Procedures.**
   a) **Device Management**

i) To control desktop and network access, all KDHE desktops shall implement an automated password protected screen saver when not in use.
ii) KDHE OITS must have and maintain an Information Technology Security Incident Policy to protect against a Cyber-attack, which is any attack on any part of the IT infrastructure. This policy should be reviewed annually to ensure that the procedures are up-to-date.
iii) KDHE must implement a computer device security and testing evaluation process to ensure systems, servers, databases and devices meet a minimally acceptable level of security.

**b) Access Control**

i) KDHE uses access controls and other security measures to protect the confidentiality, integrity and availability of information handled by computer and communication systems.
ii) Access to KDHE data and information resources (excluding web mail) from external networks will not be permitted unless the security of the information and the system can be assured.
iii) KDHE OITS has the responsibility to ensure the integrity of all data and configuration controls.
iv) Security of all data is maintained through mandatory access controls.
v) Equipment that is not owned by KDHE cannot be attached to the internal KDHE computer network without prior authorization from KDHE OITS. This includes equipment used by vendors and non-KDHE personnel for demonstrations and equipment received by KDHE for testing and proof-of-concept purposes.
vi) Vendors or Vendors shall establish and maintain appropriate administrative, technical and physical safeguards to protect the security of the data in their systems, and must prevent unauthorized access to it.
vii) Vendors or Vendors shall not disclose, release, show, sell, rent, lease, loan or otherwise have access granted to the data covered by KDHE agreement to any person not involved with the project.
viii) The KDHE information processing facilities must be in a locked location with only authorized personal having access.
ix) KDHE information must be consistently protected in a manner proportionate with its sensitivity, value and criticality.
x) The information in the form of a computer file, diskette, paper, verbal or any other falls in one of the two following categories: a) Restricted or b) Public.
xi) KDHE employees must identify requestors of information and make certain that their requested use of KDHE information is authorized under the Kansas Open Records Act or KDHE business agreements.
xii) KDHE restricted or private data must be shared only for purposes expressly authorized by the Kansas Open Records Act and agency management.
xiii) Data owners shall execute agreements regarding the protection of information between any entity providing access to information either by computer file, diskette or paper.
xiv) Data owners must authorize access to any KDHE application system containing restricted, or private data, and for data sharing between applications.
xv) KDHE OITS will coordinate with KDHE data owners to establish criteria for access and user
xvi) •validation to an application containing Restricted or Private data in conformity with KDHE Information Technology Security Policy, State of Kansas Information Technology Security Policies and industry best practices
xvii) Flexibility and business needs will be balanced against security risks.
xviii) KDHE OITS has the responsibility to ensure the continued availability of data and programs to all authorized staff members.
xix) Network controls shall be implemented to protect against the highest risks. External network boundaries and key internal boundaries will be monitored and controlled by firewall(s) managed by the Security Access Administrator(s).

xx) The security administration function ensures confidentiality, integrity and availability of the information system network.

xxi) KDHE OITS Database administrators are responsible for the development, maintenance and integrity of KDHE databases unless otherwise specified by the data owner.

xxii) The application developer is responsible for ensuring that the applications they develop adhere to current industry programming best practices and to KDHE security policies.

xxiii) The application developer will work closely with the KDHE information security technical staff to ensure that controls meeting KDHE security requirements are included in application design specifications and part of the application system development.

xxiv) A security plan shall be required for all projects involving development and implementation of new systems or modifications to an existing system where there is a change in access or functionality.

xxv) Appropriate information security and audit controls shall be implemented in all new applications.

xxvi) KDHE OTIS has the responsibility to install, support, maintain and monitor the information system network.

xxvii) The KDHE Security Officer is responsible for monitoring user access and security for KDHE systems and reporting any potential breach of security to KDHE OITS management.

xxviii) KDHE authorizes the OITS staff to access its networks and/or firewalls to the extent necessary to perform vulnerability scans. To control physical access, all closets that contain network equipment (i.e. cables, routers, network switches and access points) shall be secure with the State of Kansas Network Provider controlling their access.

xxix) KDHE employees shall notify management if they detect or suspect any unauthorized use or attempted misuse of their personal authenticators, desktops or equipment.

xxx) Distribution or use of network diagnostic, monitoring, scanning tools or hardware/software attack scanners shall be limited to the KDHE Chief Information Officer's designated and authorized personnel.

xxxi) KDHE IT technical staff shall be responsible for maintaining up-to-date diagrams showing all major network components, to maintain an inventory of all major network connections and to ensure that all those unneeded are disabled.

xxxii) Default passwords on network hardware such as routers and network switches shall be changed immediately after hardware is installed. KDHE information security policies were drafted to meet or exceed the protections found in existing laws and regulations. Any KDHE information security policy believed to be in conflict with existing laws or regulations must be promptly reported to the CIO.

xxxiii) KDHE management reserves the right to revoke a user's information system privileges at any time.

xxxiv) All information system security controls must be enforceable prior to being adopted as a part of the standard operating procedure.

xxxv) KDHE management must publish written information technology security policies and make them available to all employees and relevant external partners.

xxxvi) All KDHE assets should be clearly identified and an inventory of all important assets completed and maintained.

xxxvii) KDHE should ensure that the security controls, service definitions and delivery levels included in the third party service delivery agreement are implemented, operated and maintained by the third party.

xxxviii) Statements of business requirements for new information systems or enhancements to existing systems should specify the requirements for security controls.

xxxix) The KDHE OITS will respond in writing to all requests for authorization of device use under this policy and maintain a record of such authorization with the KDHE Information Security Office.

**c) Authentication**

**i)** Data owners are responsible for authorizing access to applications containing restricted or private data as well as authorizing data sharing between applications in response to any request for access.

**ii)** The authorities to read, write, modify, update or delete information from automated files or databases shall be established by the owner(s) of the information.

**iii)** Procedures are enforced so that application IT staff is prohibited from making unauthorized program changes.

**iv)** Computer access must require a password.

**v)** Passwords must be at least seven (7) characters long and contain a capital letter, a small letter, a special character and a number.

**vi)** Passwords must be changed at least every 90 days.

**vii)** KDHE-issued computers will be configured by KDHE OITS to require a password to unlock the computer after 10 minutes of user inactivity.

**viii)** KDHE employees must keep computer passwords confidential.

**ix)** KDHE employees must avoid keeping a paper record of their computer password, unless it can be stored securely.

**x)** KDHE employee's network and computer account information must not be shared and group network or computer accounts shall not be permitted, except when required by specific applications or computer platforms, which must be approved by the KDHE Information Security Officer.

**xi)** KDHE employee's network and computer accounts will be terminated when he/she is inactive or dormant for a period of 30 days.

**xii)** KDHE employee's network and computer accounts must be immediately disabled when the user's employment is terminated, the employee transfers to a position where access is no longer required or the employee is on extended leave where access is no longer required.

**xiii)** KDHE employee's network and computer account information must be updated within a month after an employee's legal name changes.

**d) Encryption**

i) The use of encryption is required for all computers that must store or access restricted information.

ii) The use of encryption is required for the transmission of restricted information to/from KDHE computers.

**e) Incident Detection and Response**

i) KDHE's Chief Information Officer is required to develop and maintain the OITS Disaster Recovery Plan to assure the continuation of vital agency operations in the event of a disaster.

ii) A managed process should be developed and maintained for business continuity throughout the organization in the event a disaster, including the order of restoration of databases, which is determined by the Secretary of KDHE.

**f) User Responsibilities**

i) All KDHE employees must practice due diligence to protect the confidentiality, integrity and availability of all KDHE data. Misuse of KDHE data could result in termination of employment, civil or criminal charges, and rescission of any contractual arrangement or any combination thereof.

ii) All KDHE employees must use agency data only for the purposes specified by the data owner.

iii) All KDHE employees must comply with the data controls established by the data owner and the KDHE Office of Information Technology Services.

iv) All KDHE employees must obtain permission from the data owner and the KDHE Office of Information Technology Services before creating KDHE information databases and/or datasets containing Restricted Data.

v) All KDHE employees must obtain permission from the data owner before sending, copying or moving any restricted KDHE information from a secure location to a non-secure location.

vi) Agency employees must notify KDHE OITS immediately if a KDHE data item is lost or stolen. Examples of data items are: USB drives, blackberries, iPhones and iPads.

vii) KDHE users shall contact the KDHE Help Desk for device use requiring KDHE Office of Information Technology Services approval.

**4) Action.**

a) This directive applies to all computers and all computer devices issued by KDHE.

b) Any exceptions to the prescribed procedures must be approved by the KDHE Chief Information Officer.

c) Any deviation from the prescribed procedures in the Policy, the KDHE Acceptable Use Policy, the KDHE Information Technology Security Policy or other use as authorized by the KDHE OITS, subjects the user to disciplinary action, up to an including termination, under State of Kansas Personnel Policy and Procedures.

Robert Moser, M.D., Secretary
Department of Health and Environment

12/19/12
Date

**Kansas Information Technology Executive Council**

**Information Technology Policy 7400 - Computer Security Awareness and Training**

1) TITLE: Kansas IT Enterprise Policy for Computer Security Awareness and Training
   a) EFFECTIVE DATE: January 22, 2009
   b) TYPE OF ACTION: New Policy
   c) KEY WORDS: Kansas IT Security Council, Enterprise Security Policy, Information Security, User Security Awareness, Desktop User Security Training

2) PURPOSE: To ensure all Kansas government employees, Vendors, or other third parties who have access to or use Kansas IT resources, have available training and opportunities to meet and respond to computer security issues and incidents faced in the workplace.

3) ORGANIZATIONS AFFECTED: All Branches, Boards, Commissions, Departments, Divisions and Agencies of state government; *and Vendors or other third parties;* hereafter referred to as Entities.

4) REFERENCES:
   a) ITEC IT Policy 7230, Revision 1, General Information Technology Enterprise Security Policy
   b) Kansas IT Security Council, IT Security Reporting Protocols, October 25, 2007
   c) Kansas IT Security Council, IT Security Awareness and Training Policy Requirements
   d) Department of Administration, Intrusion Detection Incident Response Security Policy and Procedures
   e) NIST Special Publication 800-16, Information Technology Security Training Requirements
   f) NIST Special Publication 800-50, Building an Information Technology Security Awareness and Training Program

5) DEFINITIONS:
   a) Security incident is defined as a compromise of a system that has critical, sensitive, or confidential data; any compromise that significantly affects agency resources; the act of violating an explicit or implied security policy; the act of violating any Federal, State or local law which may result in the loss of confidentiality, integrity or availability. Compromises may be the result of failed or successful unauthorized access attempts; unwanted disruption of service; or use of a system to change or damage system hardware, firmware or software.

6) POLICY:
   a) Statement of Responsibility: The Kansas IT Security Council is responsible for establishing a minimum security standard and for tracking training via the annual Enterprise Security Self Assessment as a vehicle to promote awareness.
   b) Every state employee, Vendor or other third parties shall receive annual training according to minimum standards as set forth in section 6.1.

   c) Those agencies whose budgets fall under the $100,000 reporting criteria will be provided assistance in meeting provisions of section 6.2.
   d) Kansas Board of Regents Institutions must follow this policy or an approved industry best practices policy designed for higher education technical environments or institutions.

7) PROCEDURES:
   a) The practices and procedures for Computer Security Awareness and Training shall conform to the requirements set forth in the "Computer Security Awareness and Training Policy Requirements", as amended, included as Attachment A to this policy.

8) RESPONSIBILITIES:

a) Heads of entities are responsible for establishing procedures for their organizations to comply with the requirements of this policy.
b) Entities are responsible for developing programs to ensure employees receive user awareness training at least once yearly.
c) The Kansas IT Security Council is responsible for the maintenance of this policy.

9) CANCELLATION: None

**Information Technology Executive Council (ITEC)**
**ITEC Policy 7400A**
**Computer Security Awareness and Training Policy Requirements**

***Purpose***

Security Awareness and Training requirements identify the steps necessary to provide IT system managers, administrators, and users with awareness of system security requirements and of their responsibilities to protect IT systems and data.

***Minimum Requirements***

Each Entity shall fulfill the following responsibilities:

1. Designate an individual who is responsible for all aspects of an Entity's security awareness and training program including development, implementation, testing, training, monitoring attendance, and periodic updates.
   Note: This responsibility should normally be part of the Information Security Officer's role.

2. Include any Entity-specific IT security training requirements in the Entity IT security awareness and training program.
   Example: An Entity that processes data covered by the Health Insurance Portability and Accountability Act (HIPAA) must have an IT security training program that addresses specific HIPAA data security requirements.

3. Require that all employees, Vendors or other third parties receive IT security awareness training annually, or more often as necessary.

4. Provide additional role-based IT security training commensurate with the level of expertise required for those employees, Vendors or other third parties who manage, administer, operate, and design IT systems, as practicable and necessary.
   Example: Entity employees and Vendors who are members of the Disaster Recovery Team or Incident Response Team require specialized training in these duties.

5. Implement processes to monitor and track attendance at IT security training.

6. Require IT security training as part of new employee orientation and thereafter on a yearly basis for the user to have) IT system users access rights to the Entity's IT systems, and in order to maintain these access rights.

7. Develop an IT security training program so that each IT system user is aware of and understands the following concepts:
   - Passwords including creation, changing, aging and the need to keep confidential.
   - Privacy and proper handling of sensitive information
   - Physical Security
   - Social Engineering
   - Identity theft avoidance and action
   - Email usage
   - Internet usage
   - Viruses and malware
   - Software usage, copyrights and file sharing
   - Portable devices
   - Proper use of encryption devices
   - Reporting

a. Suspicious activity
b. Abuse

8. Require documentation of IT system users' acceptance of the Entity's security policies after receiving IT security training